(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09121340 A**

(43) Date of publication of application: **06 . 05 . 97**

(51) Int. Cl **H04N 7/173**
G09C 1/00
H04L 9/32
H04N 7/167

(21) Application number: **08176892**

(22) Date of filing: **05 . 07 . 96**

(30) Priority: **07 . 07 . 95 US 95 499280**

(71) Applicant: **THOMSON CONSUMER ELECTRON INC**

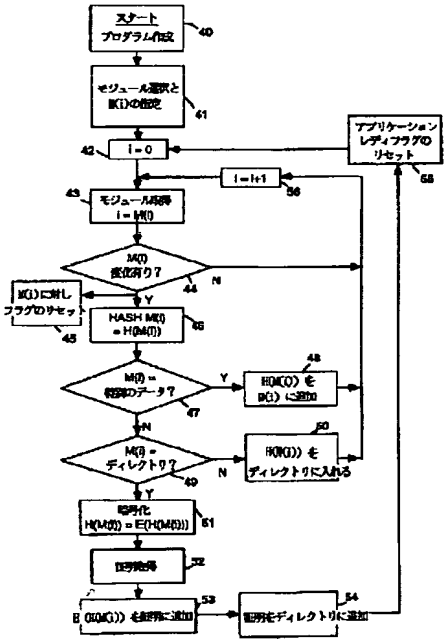
(72) Inventor: **ROHATGI PANKAJ**
DUREAU VINCENT

(54) **DEVICE AND METHOD FOR VERIFYING APPLICATION TRANSMITTED IN TWO-WAY INFORMATION SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide the receiving method and device for a 2-way television system to receive only permitted data.

SOLUTION: A 2-way program is coupled with transmission audio/video data, resulting data are divided into modules and a directory module to kink the modules is generated 49. Security of an application is obtained by addition of signed certificate to each directory and the completeness of a module is monitored by applying hash processing to each module and storing the hashed value to the directory. The hashed value of the directory including other hash values is ciphered and added to the directory 54. The certificate is decoded by receiver, a certificate of a provider is checked and a program is executed so long as the has value of each program generated by a receiver matches a corresponding to has value of the directory when the certificate is verified.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－121340

(43)公開日　平成９年(1997)５月６日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
Ｈ０４Ｎ	7/173			Ｈ０４Ｎ	7/173		
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｂ	
			7259－5Ｊ			６４０Ｅ	
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７５Ｂ	
Ｈ０４Ｎ	7/167			Ｈ０４Ｎ	7/167	Ｚ	

審査請求　未請求　請求項の数23　ＯＬ　（全 23 頁）

(21)出願番号　特願平8－176892

(22)出願日　平成８年(1996)７月５日

(31)優先権主張番号　４９９２８０

(32)優先日　1995年７月７日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　391000818
トムソン　コンシューマ　エレクトロニクス　インコーポレイテッド
THOMSON CONSUMER ELECTRONICS, INCORPORATED
アメリカ合衆国　インディアナ州　46290－1024　インディアナポリス　ノース・メリディアン・ストリート　10330

(74)代理人　弁理士　伊東　忠彦　（外１名）

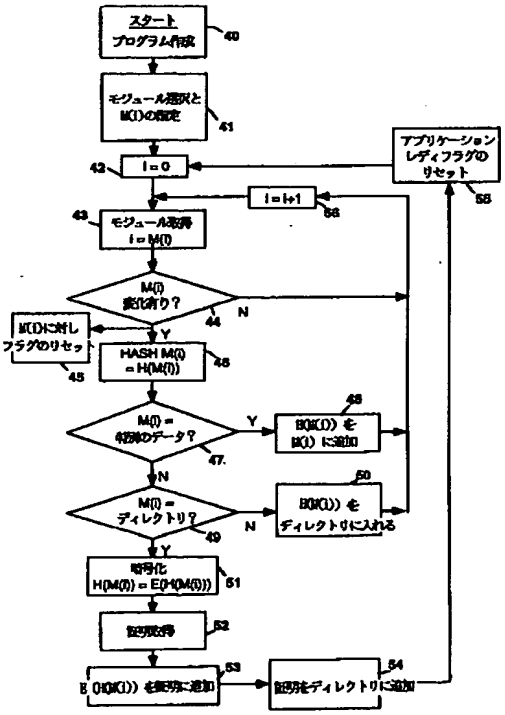
最終頁に続く

(54)【発明の名称】　双方向情報システムにおいて伝送されたアプリケーションを認証する装置及び方法

(57)【要約】

【課題】　本発明は、許可されたデータだけを受ける双方向テレビジョンシステムの受信方法及び装置の提供を目的とする。

【解決手段】　双方向番組が伝送用オーディオ／ビデオデータと結合され、モジュール分割され、モジュールを連結するディレクトリモジュールが作成される。アプリケーション秘密性は各ディレクトリへの署名付き証明の添付により得られ、モジュール完全性はモジュールをハッシュし、ハッシュ値をディレクトリに格納して監視される。他のハッシュ値を含むディレクトリのハッシュ値が暗号化されディレクトリに添付される。証明が受信器で復号化され、プロバイダ認証が検査され、証明が認証されたとき、受信器が作成した各プログラムのハッシュ値がディレクトリの対応ハッシュ値と一致する場合に限り、番組が実行可能である。



1

【特許請求の範囲】

【請求項１】　少なくともディレクトリモジュールに関する暗号化されたハッシュの値と、アプリケーションプロバイダの身分証明を含む付加的な暗号化された証明とを有し、他のモジュールに関する情報を格納するディレクトリモジュールが含まれているモジュールで伝送された実行可能なアプリケーションを受信する装置であって：メモリと；伝送された該モジュールを検出し、検出されたモジュールをメモリに記憶する検出器と；検出されたディレクトリモジュールから該証明を分離する手段と；該証明及び該暗号化されたハッシュの値を解読する解読器と；別のハッシュの値を作成するため、検出された該ディレクトリモジュールをハッシュするハッシュ関数素子と；解読された該証明を認証し、解読された該ハッシュの値を該別のハッシュの値と比較し、解読された該ハッシュの値と該別のハッシュの値が一致し、かつ、該証明が認証されたとき、プログラムの実行を許可するようプログラムされたプロセッサとからなる装置。

【請求項２】　該ディレクトリモジュールは、別のプログラムモジュールのハッシュの値を更に有し、
該ディレクトリモジュールから検出された該別のプログラムモジュールのハッシュの値をアクセスする手段と；該別のプログラムモジュールに関するハッシュの値を生成するため夫々の該別のプログラムモジュールを該ハッシュ関数素子に供給する手段とを更に有し、
該プロセッサは、該ディレクトリモジュールから得られた別のプログラムモジュールの該ハッシュの値を該ハッシュ関数素子によって作成された対応するハッシュの値と比較し、対応するハッシュの値の中の少なくとも所定のハッシュの値が一致するならば、該プログラムの実行を許可するよう条件付けられている、請求項１記載の装置。

【請求項３】　伝送された該ディレクトリモジュールが暗号化され、
該解読器は、該アプリケーションプロバイダの公開鍵で該ディレクトリモジュールを解読するよう条件付けられている請求項１記載の装置。

【請求項４】　該プロセッサが対応するハッシュの値が一致しないモジュールを該メモリから削除する手段を有する請求項２記載の装置。

【請求項５】　該解読器及び該ハッシュ関数素子が該プロセッサ内に含まれている請求項１記載の装置。

【請求項６】　該検出器が前方誤差補正回路を含む請求項１記載の装置。

【請求項７】　伝送された該実行可能なアプリケーションは、サービスチャンネル識別子とスクランブルフラグとを含む各伝搬パケットで送信され、
該検出器は、多重化された伝搬パケットのストリームから所定のサービスチャンネル識別子を有する伝搬パケットを選択するプログラム可能なサービスチャンネル識別子検出器を含み、
該スクランブルフラグに応答し、該スクランブルフラグの状態に従って夫々のパケットのスクランブルを解除するスクランブル解除器を更に有する請求項１記載の装置。

【請求項８】　認証されていないアプリケーションプロバイダによって提供された信号の検出を知らせる表示を発生する手段を更に有する請求項１記載の装置。

【請求項９】　所定のテキストのディジタルバージョンのソースと；上記ディレクトリモジュールを含む少なくとも一つの該モジュールを該所定のテキストのディジタルバージョンで始める手段とを更に有し、
該ハッシュ関数素子は、該所定のテキストのディジタルバージョンで始められた該少なくとも一つのモジュールをハッシュするよう条件付けられている、請求項１記載の装置。

【請求項１０】　該所定のテキストは、ＯＰＥＮＴＶ（登録商標）である請求項９記載の装置。

【請求項１１】　該ディレクトリモジュールは、モジュローＮ及び冪指数ｅのＲＳＡアルゴリズムを用いて計算された署名Ｓと、上記モジュローＮによる除算によって上記署名Ｓから得られた商Ｑ１及びＱ２とを含み、
該プロセッサは、算術的除算を行なうことなく上記商Ｑ１及びＱ２を用いて該署名Ｓを照合するよう条件付けられている、請求項１記載の装置。

【請求項１２】　別々のアプリケーションのモジュールを連結する情報を格納し、かつ、アプリケーションのプロバイダに関する情報を含み、システムプロバイダの秘密鍵によって暗号化された証明が添付されたディレクトリモジュールを含むモジュールとして、多重化されたパケットフォーマットで伝送された実行可能なアプリケーションを処理する方法であって、
所望のアプリケーションを含むパケットを検出、選択し、夫々のパケットのペイロードを夫々のモジュールとして記憶する段階と；暗号化された証明が添付されたディレクトリモジュールを選択する段階と；上記証明を上記システムプロバイダの公開鍵で解読する段階と；解読された該証明の情報を対応する記憶されたデータと比較する段階と；モジュールのハッシュの値を作成するため、該アプリケーションモジュールの中のモジュールをハッシュする段階と；該モジュールのハッシュの値を、該ディレクトリモジュールで伝送された対応するモジュールのハッシュの値と比較する段階と；作成され、伝送された対応するハッシュの値が一致し、かつ、該証明に格納された解読された情報が該対応する記憶されたデータと一致する場合に、アプリケーションを実行する段階とからなる方法。

【請求項１３】　該証明はアプリケーションプロバイダの公開鍵を含み、該ディレクトリモジュールは、該アプリケーションプロバイダの秘密鍵で暗号化された添付さ

れた該ディレクトリモジュールのハッシュの値を有し、解読された該証明から該アプリケーションプロバイダの公開鍵を取り出し、該ディレクトリモジュールから暗号化された該ハッシュの値を分離する段階と；暗号化された該ハッシュの値を該アプリケーションプロバイダの公開鍵を用いて解読する段階と；解読された該暗号化されたハッシュの値を検出された該ディレクトリモジュールのハッシュの値と比較する段階とを更に有する請求項１２記載の方法。

【請求項１４】　該ディレクトリモジュールをハッシュする前に、ディジタル形式の上記テキストＯｐｅｎＴｖ（登録商標）を該ディレクトリモジュールに追加する段階と、

該ディジタル形式の上記テキストＯｐｅｎＴｖ（登録商標）が追加された該ディレクトリモジュールをハッシュする段階とを更に有する請求項１２記載の方法。

【請求項１５】　実行可能なアプリケーションを生成し、該アプリケーションを、該アプリケーションの一部分を含むモジュールと、アプリケーション内のモジュールを連結する情報を含むディレクトリモジュールとに形成するプロセッサと；対応するハッシュの値を作成するため、該アプリケーションのモジュール上で一方向のハッシュ関数を実行し、該ハッシュの値を該ディレクトリモジュールに挿入するため該プロセッサと協働するハッシュ関数素子と；アプリケーションプロバイダの公開鍵と、システムコントローラの秘密鍵で署名され、アプリケーションプロバイダの識別子と上記証明の作成の時間及び満了の時間の一方に関係したタイムスタンプを含む証明のソースと；該アプリケーションプロバイダの公開鍵及び該証明を該ディレクトリモジュールに添付する手段と；該アプリケーションの該モジュールで時分割多重化された信号を形成する伝搬プロセッサとからなる、実行可能なアプリケーションを送信する装置。

【請求項１６】　該アプリケーションモジュールのハッシュの値を含む該ディレクトリモジュールのハッシュの値を、該アプリケーションプロバイダの秘密鍵で暗号化する暗号化装置と；該ディレクトリモジュールの暗号化された該ハッシュの値を該ディレクトリモジュールに添付する手段とを更に有する請求項１５記載の装置。

【請求項１７】　該モジュールの中には該アプリケーションの実行中にデータが変わることが期待されるデータモジュールがあり、該プロセッサは、夫々のモジュールにバージョン番号を付け、上記モジュールが変化したとき、モジュールのバージョン番号を変更し；該ハッシュ関数素子は、新しいハッシュの値を作成するため各変更されたモジュールのバージョン番号をハッシュし、該新しいハッシュの値を対応するモジュールに添付するため該プロセッサと協働する、請求項１５記載の装置。

【請求項１８】　所定のテキストのディジタルバージョンのソースと；該所定のテキストの該ディジタルバージョンを該ディレクトリモジュールで多重化するマルチプレクサとを更に有し、

該ハッシュ関数素子は、所定のテキストの該ディジタルバージョンと上記ディレクトリモジュールの組み合わせをハッシュするよう条件付けられている、請求項１５記載の装置。

【請求項１９】　実行可能なアプリケーションを生成し、モジュールに分割する段階と；夫々のアプリケーションモジュールを連結する情報を含むディレクトリモジュールを形成する段階と；夫々のモジュールに対しハッシュの値を生成するため、一方向のハッシュ関数で夫々のモジュールをハッシュする段階と；夫々のモジュールに対するハッシュの値を該ディレクトリモジュールに格納する段階と；システムコントローラの秘密鍵で暗号化されたアプリケーションプロバイダの身分証明を含む証明にアクセスする段階と；上記証明を該ディレクトリモジュールに添付し、該アプリケーションを送信する段階とからなる実行可能なアプリケーションを送信する方法。

【請求項２０】　ディレクトリモジュールのハッシュの値を生成するため、上記ディレクトリモジュールをその中に含まれているハッシュの値でハッシュする段階と；上記ディレクトリモジュールのハッシュの値を暗号化する段階と；暗号化された該ディレクトリモジュールのハッシュの値を該ディレクトリモジュールに添付する段階とを更に有する請求項１９記載の方法。

【請求項２１】　第三者的プロバイダの身分証明を含む別の証明を生成する段階と；上記別の証明を上記アプリケーションプロバイダの秘密鍵で暗号化する段階と；暗号化された該別の証明を該ディレクトリモジュールに添付する段階とを更に有する請求項１９記載の方法。

【請求項２２】　該ディレクトリモジュールをアプリケーションプロバイダの秘密鍵で暗号化し、該暗号化されたディレクトリモジュールを送信する段階と；残りのアプリケーションモジュールを平文で送信する段階とを更に有する請求項２０記載の方法。

【請求項２３】上記ハッシュの値を該ディレクトリモジュールに格納する段階は、１２８ビット長からなる夫々のハッシュの値を格納し、

上記証明を該ディレクトリモジュールに添付する段階は：３２ビットの証明記述子又はフラグと、３２ビットの識別子と、３２ビットの期間満了記述子と、３２ビットのファイル記憶容量限界と、１２８ビットの名前と、３２ビットの公開鍵とからなる証明を添付する段階を有する、請求項１９記載の方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、双方向テレビジョンシステム（ＩＴＶＳ）により受けられたデータが許可されたデータであることを保証する方法及び装置に関す

る。

【０００２】

【従来の技術】双方向テレビジョン（ＴＶ）システムは、例えば、米国特許第５，２３３，６５４号明細書によって周知である。双方向テレビジョンシステムは、典型的に、プログラミング及び／又は制御データ（以下、ＰＣ－データと呼ぶ）と、オーディオ及びビデオ情報を夫々の受信装置に伝送することに係る。受信装置は、受像器が自動的に使用、或いは、受信器のユーザが選択的に使用するため、ＰＣ－データを復号化し、ある種の制御装置に供給する。制御装置は、例えば、コンピュータの形式でもよく、その用途には、例えば、引き続くユーザの操作のため財政上のデータをダウンローディングすることが選択的に含まれている。

【０００３】双方向テレビジョンシステムの情報は圧縮されたディジタル形式で伝送されると考えられる。システムの受信端には、伝送された情報の受信及び圧縮解除を行い、復号化されたオーディオ、ビデオ及びＰＣ－データを夫々のプロセッサに供給する統合形の受信器の復号化器（ＩＲＤ）が含まれている。オーディオ及びビデオプロセッサは、オーディオ及びビデオ再生装置又はテレビジョン受像機でもよく、ＰＣ－データプロセッサはコンピュータでも構わない。理想的には、システムは、許可されたサービスプロバイダーによって提供された十分にテストされたＰＣ－データだけを供給し、かかる条件下で伝送された情報が夫々の受信器に実際に害を与える可能性は殆どない。

【０００４】

【発明が解決しようとする課題】しかし、多数のプロバイダーが上記システムの使用を許可された場合、システムは、ａ）許可されていないユーザによる侵入、システムユーザに対する意図的な損害の付与、ｂ）不注意のＰＣ－データの準備及びその結果によるシステムユーザへの故意でない損害の被害を受けやすくなる。何万ものＩＲＤに同時にＰＣ－データを送信する能力は、性質の悪いソフトウェアによってもたらされる可能性のある潜在的な破壊を多重に増倍させる。かくして、性質が悪く、かつ、許可されていないＰＣ－データから夫々のＩＴＶＳ受信器を確実に保護する手段が必要である。

【０００５】

【課題を解決するための手段】本発明の受信器の実施例は、ＰＣ－データの信号パケットを選択するため伝送された番組ガイドに応答するＩＲＤを含む。ＩＲＤは選択されたＰＣ－データを一時的に記憶する。許可されたＰＣ－データは証明を含む。ＰＣ－データプロセッサは、証明を分離し、認証のためその証明を検査するように構成されている。上記プロセッサは、ＰＣ－データの一部分をハッシュし、生成されたハッシュの値を、ＰＣ－データと共に伝送され、ＰＣ－データの同一部分に対応するハッシュの値と比較する。ハッシュの値が一致し、証明が認証された場合、システムは伝送された番組を実行するよう条件付けられる。

【０００６】送信器の実施例は、双方向番組を提供するためのソフトウェア生成装置を含んでいる。番組はモジュールに分割され、ディレクトリモジュール(Directory Module)が生成される。夫々のモジュールがハッシュされ、生成されたモジュールのハッシュの値がディレクトリモジュールに格納される。上記モジュールは、次に、送信のため条件付けされる。

【０００７】

【発明の実施の形態】以下、添付図面を用いて本発明の説明を行なう。例えば、直接放送衛星システムのような圧縮ディジタル伝送システムの環境で本発明を説明する。単一の衛星トランスポンダは、時分割多重化フォーマットで複数のＴＶ番組の各々に適応すると考えられる。

【０００８】図１を参照すると、パケットマルチプレクサ１６は、その出力ポートに、オーディオ－ビジュアル－インタラクティブ（ＡＶＩ）番組を供給する。同様のパケットマルチプレクサ２６は、代わりのＡＶＩ番組を発生する。サービスチャンネル識別子（ＳＣＩＤ）を介して夫々のＡＶＩ番組のオーディオ、ビデオ及びインタラクティブ成分に関係した情報を含む番組ガイドは、処理素子２７によって、ＡＶＩ番組に類似した伝送フォーマットで提供される。番組ガイド及び各ＡＶＩ番組は、伝搬パケット形式でチャンネルマルチプレクサ２８の各入力ポートに供給される。チャンネルマルチプレクサ２８は、各パケット信号を単一の信号ストリームに均等に時分割多重化するための周知の構造でもよく、或いは、統計的に制御されたマルチプレクサでもよい。マルチプレクサ２８の出力は、リード－ソロモン及びトレリス符号化器を含む前方誤差符号化（ＦＥＣ）信号インターリーブ装置３１に接続される。前方誤差符号化器３１の出力はモデムに結合され、多重化された信号が、例えば、衛星トランスポンダに対するアプリケーションのため条件付けられる。統計的に多重化されたパケット信号の一例が図２に示され、各パケットに対するフォーマットの一例が図３に示されている。

【０００９】ＡＶＩのフォーマット化は、システム番組コントローラ５によって制御される。番組コントローラ５は、特定の番組及び各番組の信号成分を選択するため用いられるユーザインタフェースを有する。番組コントローラは、各サービスチャンネル識別子ＳＣＩＤを各プログラムの夫々のオーディオ、ビデオ及びインタラクティブ成分に割り当てる。ＡＶＩ番組の構成要素に関係しているサービスチャンネル識別子ＳＣＩＤを判定し、次いで、関連したサービスチャンネル識別子ＳＣＩＤを含む伝送された信号ストリームから伝搬パケットを選択するため、各受信器が番組ガイドにアクセスする場合を想定する。オーディオ、ビデオ及びインタラクティブ成分

は、別々のサービスチャンネル識別子ＳＣＩＤが割り当てられるので、一つのＡＶＩ番組の中の少なくとも一つの成分が、代わりのＡＶＩ番組のフォーマット化の際に利用される。別々のサービスチャンネル識別子ＳＣＩＤを用いることにより、一つの番組からのオーディオを別の番組からのビデオ等と容易に編集できるようになる。

【００１０】所定のＡＶＩ番組は、多数の信号成分ソースを有する。図１に示されているように、インタラクティブ成分のソース１０と、ビデオソース１７と、第１及び第２のオーディオソース２０及び２３（二カ国語音声）。コントローラ５は、時間管理及び／又は機能の許可のため夫々のソースと通信する。ビデオ信号ソース１７は、動画像専門家グループ（ＭＰＥＧ）によって奨励されたビデオ圧縮規格に準拠して信号を圧縮するビデオ信号圧縮器１８に結合される。同様に、ソース２０及び２３からの夫々のオーディオ信号は、夫々の圧縮器２１及び２４に共有される。上記圧縮器は、動画像専門家グループ（ＭＰＥＧ）によって奨励されたオーディオ圧縮規格に準拠して夫々のオーディオ信号を圧縮する。ＭＰＥＧ方式のプロトコルに従って圧縮された関連したオーディオ及びビデオ信号は、タイミング素子１５によって供給される表示タイムスタンプ（ＰＴＳ）の使用と同期させられる。オーディオとビデオが時間的に関連付けられる様子を知るため、国際標準化機構(INTERNATIONAL ORGANIZATION FOR STANDARDIZATION), ISO/IEC JTSC1/SC 29/WG11; N0531, 動画像と関係するオーディオの符号化(CODING OF MOVING PICTURES AND ASSOCIATED AUDIO), MPEG93, 1993年 9月を引用する。

【００１１】圧縮されたオーディオ及びビデオ信号は、伝搬パケット形成器又はプロセッサ１９、２２及び２５に供給される。オーディオ及びビデオ伝搬プロセッサは周知であり、その説明は行なわない。パケットプロセッサは、圧縮されたデータを所定バイト数のペイロードに分割し、図３に示されているようにサービスチャンネル識別子ＳＣＩＤを含む識別用ヘッダを添付することだけを説明しておく。ビデオ信号伝搬パケットプロセッサに関するより詳しい情報のため、米国特許第５，１６８，３５６号明細書を引用する。パケットプロセッサは、信号成分を時分割多重化するパケットマルチプレクサに接続されている。伝搬パケットプロセッサは、マルチプレクサを他の成分のため機能させるべく、パケット化されたデータを一時的に記憶するバッファメモリを含む場合がある。パケットプロセッサは、パケットが利用可能な時点を示すためマルチプレクサに接続されたパケットレディＰＡＣＫＥＴ　ＲＥＡＤＹ信号線を含む。

【００１２】双方向番組が、コンピュータ又はパーソナルコンピュータ（ＰＣ）であるインタラクティブ成分ソース又はプログラミング素子１０を操作するプログラマによって周知の技術を用いて作成される。アプリケーションを形成する際に、プログラミング素子１０は、メモリ１１及びメモリコントローラ１２と接続され、完成したアプリケーションがメモリ１１に記憶される。完成後、アプリケーションは、信号の帯域幅を節約するため、修飾のない符号に圧縮又は翻訳される。

【００１３】アプリケーションをフォーマット化する際に、番組の一部が、図４に示されたようにモジュール、伝送ユニット及びパケットに形式化される。パケットは、上記伝搬パケットと同じ形式である。伝送ユニットは、複数の伝搬パケットにより構成される。各伝送ユニットは、伝送ユニットの内容を表わす情報を含むヘッダパケットと、アプリケーションの符号語の一部を個々に含む複数の基本パケットとを含んでいる。モジュールは、別々のモジュールからの情報のインターリーブを容易に行なうため、二つの伝送ユニットに分割される。好ましくは、伝送ユニットのインターリーブが許可されるが、別々の伝送ユニットからの伝搬パケットのインターリーブは許されない。アプリケーション及び伝送ユニット等をより詳細に説明するため、米国特許第５，４４８，５６８号明細書を引用する。

【００１４】モジュールは、コンピュータファイルと類似し、種々のタイプからなる。第１のモジュールのタイプは、各伝送ユニット及びモジュールをアプリケーションとして相互に関係付けるための情報を格納しているディレクトリモジュールＤＩＲＥＣＴＯＲＹ　ＭＯＤＵＬＥである。第２のモジュールタイプは、アプリケーションを作動又は実行するため受信器でコンピュータをプログラムするのに必要な実行可能なコードからなるコードモジュールＣＯＤＥ　ＭＯＤＵＬＥである。第３のモジュールタイプは、データモジュールＤＡＴＡ　ＭＯＤＵＬＥである。データモジュールは、アプリケーションの実行中に使用される実行不能な“データ”を含む。データモジュールは、コードモジュールよりもダイナミックである傾向があり、即ち、データモジュールは番組中に変化し、一方、コードモジュールは一般的に変化しない。第４のモジュールタイプは、信号モジュールＳｉｇｎａｌ　Ｍｏｄｕｌｅと呼ばれる。このモジュールは、例えば、ビデオのアプリケーション番組の特定の場面との同期のため、受信器の中断をトリガーし、アプリケーションの動作を中止し、或いは、番組の動作を再起動する等々のため利用される情報を含む特殊なパケットである。同期は、表示タイムスタンプを取り入れることによって行なわれる。データ、ディレクトリ、コード及び信号モジュールは、プログラミング及び／又は制御データ（ＰＣ－データ）の例である。

【００１５】各モジュールは、プログラミング素子１０によって誤って符号化される場合がある。例えば、全モジュールが、巡回冗長符号化ＣＲＣを受け、誤り検査ビットがモジュールの最後に追加される。各伝送ユニットＴＵは、伝送ユニットに関する情報を含むヘッダで構成される。図５の表Ｉには、各伝送ユニットＴＵヘッダパ

ケット内に含まれた情報のタイプの例が示されている。ヘッダにはバージョン番号が含まれている。バージョン番号は、ＡＶＩ番組の表示中にアプリケーションに変更が加えられた時点を示すため含まれる。受信器の復号化器は、バージョン番号の変化の検出に応答して実行中のアプリケーションを更新するため配置される。モジュールＩＤは、コンピュータのファイル識別子と同じであり、アプリケーションプログラマによって与えられる。モジュール伝送ユニットバイトオフセット（Ｍｏｄｕｌｅ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｕｎｉｔ　Ｂｙｔｅ　Ｏｆｆｓｅｔ）は、伝送ユニットＴＵのペイロードの第１のコード／データバイトのモジュール内におけるバイト位置を示す数である。伝送ユニットバイト長（Ｌｅｎｇｔｈ　（ｂｙｔｅ）　ＯｆＴｒａｎｓｍｉｓｓｉｏｎ　Ｕｎｉｔ）は、伝送ユニットＴＵのサイズ及び／又は伝送ユニットＴＵ内の最後のコード／データバイトの位置を示している。

【００１６】図６の表IIは、ディレクトリモジュール内に含まれている各データのタイプを示している。ディレクトリモジュールは、アプリケーション識別子ＡＩＤと、アプリケーションタイプを示すフィールドと、タイプ限定子を含むフィールドと、アプリケーションを記憶及び実行するため要求される記憶容量を示すフィールドと、アプリケーションに含まれているモジュール数を示すフィールドと、認証データのような保護データを含むフィールド（第１の保護情報ＦＩＲＳＴ　ＳＥＣＵＲＩＴＹ　ＩＮＦＯＲＭＡＴＩＯＮ）とからなるヘッダを有する。上記各フィールド、又は、以下のフィールドは、記載された順番に現れる必要はない。ディレクトリモジュールのデータ部には、各モジュールに対するヘッダデータと類似した各モジュール毎のデータが含まれている。その上、アスキーフォーマットの各アプリケーションモジュール名のリストである文字列の表がある。各モジュールに対するデータ部には、各モジュールに関連付けられた保護データ用のフィールド（更なる保護情報ＦＵＲＴＨＥＲ　ＳＥＣＵＲＩＴＹ　ＩＮＦＯＲＭＡＴＩＯＮ）が含まれる。或いは、このデータは、より汎用的なディレクトリ情報と共に、第１の保護情報フィールドに格納してもよい。以下、モジュール保護情報フィールドの内容を詳細に説明する。

【００１７】伝搬パケットのフォーマット化のため、インタラクティブ成分ソース１０は、実際の伝送ユニットを発生し、パケットを伝達するようプログラミングされるが、図１の実施例の場合、別個のコード／データパケットプロセッサ１４が含まれている。コード／データパケットプロセッサは、メモリコントローラ１２を介してメモリ１１の夫々の領域をアクセスし、夫々のアプリケーションを表わすシーケンスでパケットを発生する（図＊４を参照のこと）。

【００１８】パケットマルチプレクサ１６は、特定のスケジュールに従ってパケットを提供するため配置されている。上記スケジュールは、ＡＶＩ成分の帯域幅の要求条件によって名目的に決められる。各ＡＶＩ成分の間で接続が多重化される場合、殆ど出現することがないパケットを備えた信号成分に、より高い多重化優先順位が割り当てられる。

【００１９】多重化は完成した技術であり、ディジタル信号処理の分野の当業者は上記特定の要求条件を満たすマルチプレクサを容易に設計することができるので、パケットマルチプレクサ１６の特性の説明は行なわない。パケットマルチプレクサ１６は、入力ポートが各成分信号に接続され、かつ、出力ポートがマルチプレクサの出力ポートに接続されたスリーステート論理スイッチを用いて配置可能であるということだけを説明しておく。コントローラ５によって確立された優先順位と、パケット形成器によって与えられた夫々のパケットレディ信号とに応じて、論理スイッチを制御するため状態機械を配置してもよい。

【００２０】ＡＶＩシステムにおける保護は、ＡＶＩシステムコントローラによって実現された技術の間の精密な完全性と、全てのＡＶＩシステムに準拠する受信器内の保護コードとに基づいている。上記保護は、リベスト(Rivest)と、シャミール(Shamir)と、アドルマン(Adleman)によるＲＳＡアルゴリズム、又は、データ暗号化標準ＤＥＳを用いる公開鍵暗号法に基づいている。本発明に好ましいアルゴリズムは、モジュローと冪指数が夫々４（８ビット）バイトの倍数であるＲＳＡアルゴリズムである。一般的なタイプの秘密保護は、ディレクトリモジュールで提供される証明と、他の夫々のアプリケーションモジュールに関し生成されたハッシュの値の認証に帰する。

【００２１】ＲＳＡプロトコルの特別のクラスは、公開冪指数が３である。以下に説明するタイプの“補助”情報を包含することにより署名の検査速度が促進されるという利点が得られる。受信器が、公開モジュロー及び冪指数が夫々Ｎ及び３であるとき、ＳはデータＤに対するＲＳＡ方式の署名であることを照合する場合を想定する。照合のため、受信器は、$S^3=D\ (mod\ N)$であることを必ず示す必要がある。このため、名目上、計算法的に複雑であり、かつ、消費時間が長いＮによる除算／モジュロー演算が必要である。乗算の方が、計算法的に単純かつ高速な演算であるので、除算ではなく、乗算に基づく検査演算によって演算速度が著しく高められる。

【００２２】以下の式：

$S^3=D\ (mod\ N)$ならば、

$S^2/N=Q1+R1$；　$S*R1/N=Q2+R2$；　$R2=D$

のように定義された商Ｑ１及びＱ２を想定する。即ち、値Ｑ１及びＱ２は、Ｎによる除算によって署名から得られた整数の商である。Ｒ１及びＲ２は、夫々、除算後の剰余である。最大Ｔビットのサイズの Ｎ、Ｓ及びＤが、Ｓ＜Ｎ　及び　Ｄ＜Ｎ　であるならば、最大Ｔビットのサイズの商Ｑ１、Ｑ２が存在し、以下に概説するアルゴリズムを用いて、$S^3=D$（ｍｏｄ　Ｎ）を照合する。値Ｑ１及びＱ２が（例えば、非実時間的に）アプリケーションプログラマによって計算され、かつ、署名Ｓと共にディレクトリモジュールに伝送された場合、署名に対する高速検査が以下の如く行なわれることが分かる。

【００２３】受信器において、ディレクトリモジュールからＳ、Ｑ１及びＱ２が取り出され、

ステップ１．　$A=S^2$　を計算

ステップ２．　Ｂ＝Ｑ１のＮ倍　を計算

ステップ３．　Ａ＞Ｂ　を比較；

もし　Ａ＜Ｂ　ならば、処理を止め、署名は一致し得ない。

【００２４】それ以外の場合　Ａ＞Ｂ　ならば

ステップ４．　Ｃ＝Ａ－Ｂ　を計算

ステップ５．　Ｃ＜Ｎ　を比較；

もし　Ｃ＞Ｎ　ならば、処理を止め、署名は一致し得ない。それ以外の場合　Ｃ＜Ｎ　ならば

ステップ６．　Ｅ＝ＣのＳ倍　を計算

ステップ７．　Ｆ＝Ｑ２のＮ倍　を計算

ステップ８．　Ｅ＞Ｆ　を比較；

もし　Ｅ＜Ｆ　ならば、処理を止め、署名は一致し得ない。

【００２５】それ以外の場合　Ｅ＞Ｆ　ならば

ステップ９．　Ｇ＝Ｅ－Ｆ　を計算

ステップ１０．Ｇ＝Ｄ　を比較；

もし　成立しないならば、署名は一致しない。全ての算術演算は単純な乗算又は減算であることに注意が必要である。誤りのある署名の検出は、ステップ３、５、８又は１０で生じる。誤りのある署名がステップ３又は５で検出された場合、非常に僅かな計算時間しか消費されない。

【００２６】ＡＶＩ受信器は、番組の認証を判定するためにＰＣ－データと共に含まれている署名付き証明を解読すべく、各システムプロバイダの公開鍵（及び、好ましくは、補助的な商Ｑ１及びＱ２）が与えられている。番組の認証が確認されなかった場合、受信されたアプリケーションは、即座に受信器から捨てられる。かかる秘密システムの中枢は、アプリケーションプロバイダ及びシステムコントローラ又はサーバーへの固有の識別子ＩＤの割当てである。システムコントローラは、固有、例えば、３２ビットのＩＤを信用された各ＡＶＩアプリケーションプロバイダに配付し、アプリケーションプロバイダの公開鍵に対する証明を発行する。上記証明は、本質的に、アプリケーションプロバイダの公開鍵上のシステムコントローラのディジタル署名であり、証明の満了日付、プロバイダのＩＤ、及び、このＩＤを所有するアプリケーションが受信器のファイルシステムにおいて使用可能な記憶容量の限界のようなフィールドを含んでいる。システムコントローラは、複数の別個の秘密－公開鍵の対を利用し、証明には、各証明を解読するため、受信器が複数の公開鍵の中の何れの鍵を使用すべきであるかを指定するフラグが含まれている。

【００２７】アプリケーションプロバイダの証明は、名目上：証明フラグ CERTIFICATE__FLAGS （証明のタイプを指定し、システムコントローラの公開鍵フラグを含む場合がある）と；プロバイダ識別子　PROVIDER__ID （プロバイダ識別子の長さを示す）と；プロバイダ期限　PROVIDER__EXPIRE　（アプリケーションの期限を示す）と；プロバイダ認証フラグ　PROVIDER__AUTHORIZATION __FLAGS と；プロバイダ記憶容量限界　PROVIDER__STORAGE __LIMIT （割り当てられた受信器のメモリを示す）と；プロバイダ名　PROVIDER__NAME　（アプリケーションプロバイダの名前）と；プロバイダ固定証明　PROVIDER__FIXED __CERT　（プロバイダの公開鍵）とが含まれている。

【００２８】上記証明情報は、モジュロー１２８でハッシュされ、そのハッシュの値が情報に添付されている。上記証明フラグ CERTIFICATE__FLAGS は、受信器のプロセッサの特権動作へのアクセスを許可／拒絶する認証フラグを含む。以下に、フラグを介してアクセスされる特権を表わす例を列挙する：

１．　放送回線からダウンロードを受ける能力

２．　（例えば、ローカルＩＲＤのポートを介して接続された）ローカル回線からダウンロードを受ける能力

３．　（例えば、電話回線を介して）ローカル遠隔回線からダウンロードを受ける能力

４．　アプリケーションが同じプログラムの文脈中でトラックを切り換える（例えば、ビデオトラック１と２の間で切り換える）能力

５．　（例えば、ＴＶ番組又はチャンネルを変えるため）放送の接続を確立する能力

６．　ローカル接続を確立する能力

７．　遠隔接続を確立する能力

８．　外部装置を制御する能力

９．　未検査モジュールをダウンロードする能力

１０．　アプリケーションが暗号化法の特徴を使用する能力

１１．　アプリケーションがユーザ制限のあるファイルにアクセスする許可をユーザに要求する能力

１２．　遠隔的デバッギングのため、常駐ＯＣＯＤＥモニターを作動する能力

上記フラグは、プロバイダ証明と、アプリケーション認証フィールドディレクトリの両方の一部分である。アプリケーションは、特権動作の実行を許可される前に、認

証フラグを両方の場所にセットする必要がある。各受像器は、特定の特権へのアクセスを許可し、或いは、ある種の特権動作を保護するためプログラムされたボックスＢＯＸ認証マスクを不揮発性記憶装置内に含んでいる。

【００２９】各アプリケーションプロバイダは、固有の暗号化公開－秘密鍵の対を選択し、（例えば、認証された要求による）ＡＶＩシステムのコントローラによって証明された固有の公開鍵を有する。アプリケーションプロバイダは、公開鍵を選択する際に、ある種のガイドラインによって拘束される。上記拘束は受信器のハードウェアの能力に関係している。特に、末端に近い消費者電子受信器は、最低限のメモリと、比較的高性能ではないプロセッサと、認証処理速度及び時間に影響を与える要因と、公開鍵のサイズ及び形とを含んでいる。上記拘束には、例えば、公開鍵が５１２ビット以下であり、ビット数が２の冪乗である等が含まれる。

【００３０】特殊グループのＡＶＩシステム識別子ＩＤは、受信器又はシステムの保守を行なうため設計された番組のため確保される。かかるシステムＩＤは、サービスプロバイダの識別子ＩＤに添付されている。番組が特殊グループＩＤと認証プロバイダＩＤの両方を有する場合、対応する保守番組は、特定のプロバイダのＩＤに依存して、受信器の中のより秘密的な部分へのアクセスが得られる。例えば、アプリケーションプロバイダはシステムコントローラであり、添付されたアプリケーションがスマートカード内の権利の更新、又は、システム性能チェックの実行である。或いは、アプリケーションプロバイダは、衝動買いコマーシャルと関係し、番組は、プロバイダの貸方に対するユーザの借方のチェック、又は、収益の取立を容易に行なうことに関係している。一方、グループＩＤが特殊グループＡＶＩシステムＩＤではない場合、アプリケーションが利用可能な機能は、全アプリケーションが利用可能な機能に制限される。

【００３１】特定の受信器の製造者には、特定の製造者ＩＤが与えられる。製造者ＩＤを有する全てのアプリケーションは、受信器に常駐する特定の認証処理によって認証され、受信器の組立中に製造者によって実装される。製造者ＩＤを含む番組は、特定の製造者によって作成された受信器だけにアクセスし、製造者によって受信器内に組み込まれた特定の機能のセットにアクセスするよう作用する。このタイプのアプリケーションは、受信器の動作中のソフトウェアを改良するため利用される。

【００３２】特定の受信器に常駐するソフトウェア／ハードウェアを有するネットワークオペレータが存在していてもよい。ネットワークオペレータは、全てのネットワーク受信器のソフトウェア／ハードウェアへの選択的なアクセスを可能にするため、特別のＩＤが割り当てられている。ネットワークオペレータは、ネットワーク受信器のソフトウェア／ハードウェア内に常駐する専用の認証処理を含む場合がある。

【００３３】アプリケーションが特別のシステムタイプ、製造者タイプ、或いは、ネットワークタイプであるかどうかは、アプリケーションタイプ（ＡＰＰＬＩＣＡＴＩＯＮ　ＴＹＰＥ）フィールドのディレクトリモジュール（図６の表II）に示されている。アプリケーション限定（ＡＰＰＬＩＣＡＴＩＯＮ　ＱＵＡＬＩＦＩＥＲ）フィールドには、製造者又はネットワークオペレータ等を識別する情報が含まれている。

【００３４】秘密性が以下のようにアプリケーションに適用される。アプリケーションプロバイダがアプリケーションを生成し、ディレクトリモジュールを含む各モジュールを形成した後、アプリケーションの中で保護されるべき部分が決定される。如何なる場合でも、ディレクトリモジュールは保護される。更に、エントリーポイントを有する各モジュールが保護される。エントリーポイントの無いモジュールはプロバイダの考え次第で保護され、データモジュールはプロバイダの考え次第で保護される。データモジュール内のデータ部は屡々変更されるので、データモジュールが保護されている場合、符号化器及び受信器の負担になる比較的重い秘密化処理があることに注意する必要がある。従って、データモジュールは、屡々、保護無しに伝送される。保護されるべきモジュールが選択された場合、プロバイダは、秘密保護のため選択されたモジュールと、各モジュールに対する保護のモードのリストを形成し、上記リストを秘密情報のためのフィールド内のディレクトリモジュールに入れる。特定のＡＶＩシステムの場合、このモジュールは、一般的なディレクトリ情報、即ち、ディレクトリモジュールの第１の秘密情報部の中に含まれている。別のＡＶＩシステムの場合、特定のモジュールが保護されているかどうかを示す情報は、ディレクトリ内の各モジュールの別の秘密情報フィールドに格納されている。受信器のシステムプログラミングの一部は、モジュール保護情報に関しディレクトリを試験し、その情報に従って各モジュールに秘密処理を行なうルーチンを含んでいる。

【００３５】モジュール保護は幾つかの形式をとる。第１の方法は、選択されたモジュールをアプリケーションプロバイダの秘密鍵で暗号化するだけである。第２の方法は、モジュールで“ハッシュ”関数を実行し、夫々のモジュールの別の秘密情報フィールド内のディレクトリモジュールに“ハッシュ”の値を格納する。第３の方法は、モジュールでハッシュ関数を実行し、ハッシュの値をディレクトリモジュールに格納し、選択されたモジュールをアプリケーションプロバイダの秘密鍵で暗号化する。第４の方法は、選択されたモジュールでハッシュ関数を実行し、ハッシュの値をモジュールに添付し、モジュールとハッシュの値を暗号化し、暗号化されたハッシュの値のレプリカをディレクトリモジュール内に入れる。上記何れの方法の例でも、ディレクトリモジュールの秘密処理は、他の全てのモジュールが処理され、各モ

ジュールに対する秘密情報がディレクトリモジュールに収められた後に行なわれる。

【００３６】好ましい方法は、各モジュールでハッシュ関数を実行する段階と、夫々のハッシュの値をディレクトリモジュールの別の秘密情報フィールドに挿入する段階と、次いで、ディレクトリモジュールでハッシュ関数を実行する段階とからなる。ディレクトリモジュールのハッシュの値は、プロバイダの秘密鍵で暗号化される。

【００３７】信用されたアプリケーションプロバイダは、プロバイダ公開鍵、プロバイダＩＤ、証明の満了日付、場合によっては受信器のプロバイダに配分された記憶容量等の項目を含む署名付き証明が割り当てられる。上記証明はシステムコントローラの秘密鍵で署名されている。暗号化されたハッシュの値が署名付きの証明に添付され、その組み合わせがディレクトリモジュールに付け加えられる。ディレクトリモジュールと他の全てのモジュールは、平文でシステムコントローラに提供される。保護のため選択され、屡々変化するデータモジュールは、データモジュールのハッシュの値に基づくプロバイダの署名によって保護され、その署名は夫々のモジュールの一部から作られている。

【００３８】アプリケーションプロバイダが、実際上、下位のアプリケーションプロバイダのサブグループの管理者である可能性がある。この場合、アプリケーションプロバイダは、アプリケーションプロバイダの秘密鍵で署名され、サブプロバイダの公開鍵、サブプロバイダのＩＤ、証明の期限、場合によっては受信器でサブプロバイダに配分された記憶容量等を含む二次的証明を提供する。二次的証明は、アプリケーションプロバイダに割り当てられた証明と共にディレクトリモジュールに付け加えられる。

【００３９】好ましい保護モードは、伝送された情報が覗き見によって検出／解釈されることを妨げないという点で秘密性がない。しかし、保護、即ち、証明と、データのハッシュの取り込みが容易に実行できるという利点があり、データが許可されたソースから到来することが保証され、（受信器で認証された場合）受信されたデータの完全さが保証される。

【００４０】信用のないアプリケーションプロバイダ、即ち、アプリケーションの作成の際に不注意であり、ＡＶＩサービスの完全さを脅かすプロバイダは、夫々のアプリケーションに添付されるべき証明が提供されない。信用のないプロバイダによって提供されたアプリケーションは、信用のある証明機関による証明を受ける。証明機関は、アプリケーションの完全さを調査し、次いで、保護目的のため信用のないアプリケーションプロバイダのアプリケーションを処理し、最終的に、処理されたアプリケーションをシステムコントローラに送る。

【００４１】図１及び図７を参照して、秘密処理を更に説明する。図１には、ハッシュ素子２９と暗号化素子３０が別々に示されているが、しかし、ディジタル信号処理技術の当業者によれば、両方の機能は、素子１０の中に包含されたマイクロプロセッサ又はディジタル信号プロサッラＤＳＰによって実行してもよいことが容易に認められる。アプリケーションが作成された後、メモリ１１に記憶され（ステップ４０）、プログラマは秘密保護されるべきモジュールを選択／判定する（ステップ４１）。上記モジュールはインデックス（ｉ）でラベルを付けられている。ディレクトリモジュールは、最大のインデックスに割り当てられているので、最後に処理される。処理されるべき各モジュールは、“１”にセットされた“変化”フラグが割り当てられる。ＡＶＩシステムは、ＡＶＩプログラム中にアプリケーションを繰り返し送信する。名目上、コードモジュールと、あるデータモジュールは、番組中に変化のないまま保たれるが、変化するモジュール、例えば、データモジュールがある。アプリケーションの繰り返しの伝送中に、秘密のため変化しないモジュールの再処理は行なわず、実際に変化したモジュールだけを再処理することが好ましい。“変化”フラグは、番組の間隔中に変化に起因して再処理を要求するモジュールを秘密処理機能に告げるため設定される。最初、秘密保護されるべき各モジュールの“変化”フラグが変化モードに設定される。素子１０はシステムコントローラからの証明が利用可能であるかどうかを判定する。

【００４２】動作中のインデックス“ｉ”はゼロに設定され（ステップ４２）、第１のモジュールＭ（０）がメモリ１１から得られる（ステップ４３）。モジュールの“変化”フラグがテストされ（ステップ４４）、リセットされる（ステップ４５）。モジュールが先に処理され、“変化”フラグが変化の無いことを示している場合、システムはステップ５６に飛び越し、インデックス“ｉ”をインクリメントし、次のモジュールをアクセスする。“変化”フラグによって、モジュールで変化が発生したことが示されるならば、そのモジュールがハッシュ関数プロセッサ（ＨＡＳＨ）２９に供給される（ステップ４６）。特定のハッシュ関数は、各受信器に課される処理要求条件を制限するため比較的単純なまま維持される。上記関数は、好ましくは一方向関数である。ハッシュ関数は、計算法的に高速であり、かつ、解読又は破ることが極めて困難であることが要求される。ハッシュ関数の一例は、各々が１２８ビットの長さの２５６個の符号語w_rからなるベクトルWに基づいている。ハッシュ処理（ハッシュ）されるべきデータは、データの２５６個のビットエクスクルーシブブロックＤに分割され、ここで、$D=d_1, d_2, d_3, d_4, \ldots, d_{256}$
である。ハッシュ関数ＢＨ（Ｄ）は次式：

【００４３】

【数１】

17

$$BH(D) = \sum_{x=1}^{256} d_x w_x \bmod 2^{128}$$

のように定義される。もし、ｎブロックのデータＤが存在するならば、関数ＢＨ（Ｄ）の１２８ビットの長さのｎ個の値、B_1，B_2，B_3，．．．，B_nが生成される。全部のデータに対しハッシュを計算するため、中間結果B_iが以下のように結合される：$<B_i, B_j>$が１２８個のブロックB_i及びB_jを連結することにより得られた２５６の数を表わすと仮定すると、データに対するハッシュＨ（Ｄ）は、次式：

$H(D)=BH(<BH(...(<BH(<BH(<B_1,B_2>),B_3>),B_4>),...),B_n>)$

として定義される。

【００４４】或いは、関数Ｈ（Ｄ）は、以下の形式：

$H(D)=B_1 \text{ XOR } B_2 \text{ XOR } B_3 \text{ XOR } ... B_n$

でも構わない。ハッシングモジュールの好ましいハッシュ関数は、刊行物に周知の関数ＭＤ５である。ＭＤとは、メッセージダイジェスト(Message Digest)を表わし、ＭＤ５は、アール　リベスト(R. Rivest)による“ＭＤ５　メッセージダイジェストアルゴリズム(THE MD5 MESSAGE DIGEST ALGORITHM)”、ＲＦＣ　１３２１、１９９２年４月に記載されている。モジュールがハッシュされた後、番組中に変化することが期待されているかどうかを判定するため、モジュールがテストされる（ステップ４７）。変化が期待される場合、ハッシュの値Ｈ（Ｄ）はディレクトリ内に置かれず、メモリ１１に記憶されたモジュールに付け加えられる（ステップ４８）。或いは、ハッシュの値をプロバイダの秘密鍵で署名（暗号化）し、次いで、メモリ１１に記憶されたモジュールに追加してもよい。インデックスｉはインクリメントされ（ステップ５６）、次のモジュールがメモリから得られる。ステップ４７において、モジュールが変化していないと判定された場合、モジュールがディレクトリモジュールであるかどうかを判定するためテストが行なわれる（ステップ４９）。ディレクトリモジュールではない場合、モジュールＭ（ｉ）のハッシュの値Ｈ（Ｍ（ｉ））が、夫々のモジュールの第１の秘密情報フィールド又は別の秘密情報フィールド内のディレクトリモジュールに置かれる（ステップ５０）。インデックスｉがインクリメントされ（ステップ５６）、次のモジュールがメモリから得られる。

【００４５】ステップ４９において、モジュールがディレクトリモジュールであることが判定された場合、ハッシュされた値Ｈ（Ｍ（ｉ））は、暗号化器３０に供給され、ハッシュされた値は暗号化器でアプリケーションプロバイダの秘密鍵で暗号化される。必要があれば、この際の暗号化用の暗号化器にディレクトリモジュール全体を供給してもよい。証明が引き出され（ステップ５２）、暗号化されたハッシュの値が証明に追加され（ステップ５３）、ハッシュの値を含む証明がメモリ１１内

18

のディレクトリモジュールに添付される（ステップ５４）。番組の伝送の準備ができていることをデータパケットプロセッサ／番組コントローラに知らせるフラグがセットされる（ステップ５５）。システムはステップ４２に飛び越し、インデックスがゼロへリセットされる。システムは先に進み、番組の間のアプリケーションの繰り返しの伝送中に、モジュールが変化し、変化したモジュールだけが再ハッシュされたかどうかを検査する。上記の如く、アプリケーションプロバイダは、ディレクトリモジュールに追加される別の署名付きの情報／証明を含んでいてもよい。上記情報の署名は、プロバイダの秘密鍵を用いて暗号化器３０において行なわれる。

【００４６】他の実施例の場合、暗号化ステップ５１を削除してもよい。更に別の実施例の場合、全てのハッシュされたモジュールに対する全てのハッシュの値を暗号化してもよい。図１２には好ましいディレクトリモジュールのフォーマットが示されている。ディレクトリモジュールは平文中にある。ディレクトリ署名（ハッシュの値）と証明だけが暗号化され、ディレクトリ署名はプロバイダの鍵を用いて、証明はシステムコントローラの鍵を用いて暗号化される。その上、各モジュールがハッシュされたとき、かかるモジュールの各々は、ハッシュの前にテキスト“ＯｐｅｎＴｖ（登録商標）”のようなシステムコントローラ／プロバイダと関係したある所定のテキストのアスキーバージョンで始まるので、各モジュールの署名は、例えば、ハッシュの値　Ｈ（ＯｐｅｎＴｖ（登録商標）＋モジュール）であり、ディレクトリモジュール署名は、Ｈ（ＯｐｅｎＴｖ（登録商標）＋ディレクトリモジュール）の暗号化された値である。これは、ボックスＯＴＶがメモリ１１に付けられた図１において示されている。テキスト“ＯｐｅｎＴｖ（登録商標）”のディジタルバージョンがメモリ内に記憶され、そのディジタルバージョンが読み出されて、ハッシュ関数素子２９に供給されるとき、そのディジタルバージョンは夫々のモジュールと多重化される。

【００４７】図１２のディレクトリモジュールは、トムソン　コンシューマ　エレクトロニクス社によって開発されたＯｐｅｎＴｖ（登録商標）と呼ばれるＡＶＩシステムの好ましい実施例を示している。上記システムにおいて使用されている証明、公開鍵及び署名のフォーマットを以下に説明する。全ての証明、鍵及び署名は、ビッグエンディアン（ＢＩＧ－ＥＮＤＩＡＮ）フォーマットの多数のバイトフィールドを有する。アーキテクチャ依存性のない上記フォーマットは、種々の受信器のアーキテクチャの間の移植性を高める。あらゆるＯｐｅｎＴｖ方式の証明は、可変長部が後に続く固定構造の組み合わせであり、証明された公開鍵と、ＯｐｅｎＴｖ方式コントローラの署名とを含む。

【００４８】ＯｐｅｎＴｖ方式コントローラによって発行される証明には以下の二つのクラスがある。

19

クラス１．　アプリケーションプロデューサに与えられるプロデューサ（プロバイダ）証明
クラス２．　プロデューサ（プロバイダ）からのアプリケーションが秘密通信を確立し得るトランザクションサーバーに特有のサーバー（システムコントローラ）証明
その上、ユーザ証明がコントローラによって発行される。この証明はＯｐｅｎＴＶによって内部で解析される＊

証明フラグ長(CERTIFICATE__FLAGS __LENGTH)　（４バイト）
公開鍵サイズ長(PUBLIC __KEY __SIZE__LENGTH)　（４バイト）

ＯｐｅｎＴＶ方式コントローラによって発行された証明は、証明を記述する３２ビットフラグ構造で始まる。種々のフラグの位置及び意味は、以下の通りである。
【００５０】ＯｐｅｎＴＶ方式の証明の構造に対する実※

基本証明(BASIC__CERTIFICATE)　(0x80000000)

厳密には以下の３個のフラグが設定される。

サーバー証明(SERVER __CERTIFICATE)　(0x40000000)
プロデューサ証明(PRODUCER __CERTIFICATE)　(0x20000000)
ユーザ証明(USER __CERTIFICATE)　(0x10000000)

サーバー／プロデューサ証明とユーザ証明の間には、３２ビットフィールドの解釈に関して相違がある。証明がユーザ証明の外観を有する場合、フィールドの最後の１６ビットは、実際的に最初の３２ビットフィールドを含むそのサイズである。
【００５１】サーバー／プロデューサフラグに関し、第１の４ビットの試験後、証明されている実体が分かっているか、又は、証明が現在のシステムを越えた拡張であると考えられる。次の４ビットは、署名を作成するため使用されたＯｐｅｎＴＶ方式のコントローラの公開鍵を示している。この４ビットは、０乃至１５の数字Ｎを表している。もし、０＜＝Ｎ＜＝１４であるならば、Ｎ番目に組み込まれた公開鍵が使用されている筈である。もし、Ｎ＝＝１５であるならば、使用されるべき公開鍵は、外部ＥＸＴＥＲＮＡＬの信用されたチャンネルを介して受けられた最新の鍵である。システムの内部では、★

ＭＤ５によるＲＳＡ３方式(RSA__3 __WITH__MD5)　(0x00008000)
ＭＤ５によるＲＳＡ方式(RSA__WITH__MD5)　(0x00004000)

プロデューサ証明に対する最後のバイトには、現在フラグが定義されていない。サーバー証明に対する最後のバイトには、現在、サーバーが制約されているかどうかを示すため一つのフラグが定義されている。機能的な観点☆

サーバー制約(SERVER __CONSTRAINED)　(0x00000080)

プロデューサ署名の外部的に利用可能な固定部は、署名のタイプを特定する２バイトのフラグのフィールドと、◆

プロデューサ署名フラグ長(PRODUCER __SIGNATURE __FLAGS __LENGTH)
２バイト
プロデューサ署名サイズ長(PRODUCER __SIGNATURE __SIZE__LENGTH)
２バイト

現在、一つのフラグだけが意味がある補助されたフラグである。プロデューサの署名アルゴリズムが、プロデューサ証明に指定されたようにＲＳＡ__３__ＷＩＴＨ__Ｍ

20

＊ことはないが、外部の世界だけで利用可能になる。ＯｐｅｎＴＶシステムは上記証明のサイズだけを知っている。ＯｐｅｎＴＶ方式の特定の４バイトヘッダとは別に、残りの証明の構造は、秘密の状態に保つことが可能であり、標準的なＸ．５０９形の証明でもよい。
【００４９】以下に証明の共通部のサイズを記載する。

※現可能な拡張用のフラグは、基本ＯｐｅｎＴＶ証明に対し設定され；拡張部には設定されない。フラグは以下の如く定義される。

★鍵番号は増加するだけである。即ち、内部的に鍵が５であり、鍵６による証明が行なわれ、照合されたとき、内部の鍵は６になり、６未満の鍵による証明は許容されない。最後に、全ての内部の鍵が現れた場合、及び、そのとき、外部ＥＸＴＥＲＮＡＬの信用されたチャンネルからの公開鍵だけが許容される。
【００５２】次のバイトは、証明の説明のため確保されている。現在は使用されていない。次の２バイトは、証明中のプロデューサ／サーバー及び鍵に関する情報を提供する。第１のバイトは公開鍵に関するアルゴリズムを説明するフラグを含み；この第１のバイトは、サーバーとプロデューサの両方の場合に共通している。次の最後のバイトはプロデューサとサーバーに対し相違しているので、別個に説明する。
【００５３】アルゴリズムバイトフラグは：

☆から、制約されたサーバーは、最初に秘密回線を確立するとき、接続中の加入者に関する情報を必要としない。これにより、回線の確立が非常に高速化される。

◆署名のサイズを与える２バイトのフィールドとから構成される。

Ｄ５である場合、プロデューサは、高速検査のための署名の後、付加的な補助データの追加が選択可能であり、

プロデューサ署名補助(PRODUCER __SIGNATURE __ASSIST) (0x8000)

プロデューサ、サーバー及びＯｐｅｎＴＶ方式のボックスのための公開鍵構造（ＲＳＡアルゴリズム用）を以下に説明する。移植性のため、モジュロー及び冪指数のサイズは、４バイトの倍数でなければならない。更に、ＯｐｅｎＴＶ方式は、モジュローのサイズがＳバイトであるならば、モジュローの最初の３２ビットは、ビッグエンディアンフォーマットで表現されたとき、非ゼロでなければならない。サイズはＳ－４未満であると言うことができるので、このことによる制限はない。

【００５４】公開鍵は：固定公開鍵(fixed__public. __key __t)と、冪指数(exponent)（ビッグーエンディアンバイトフォーマット）と、モジュロー(modulus)（ビッグーエンディアンバイトフォーマット）とにより構成される。

【００５５】プロデューサ／サーバー証明は、上記データタイプのプロデューサ／サーバーの公開鍵が後に続く、ＯｐｅｎＴＶ方式コントローラによる証明の記述子を含む平文部分からなる。更に、ＯｐｅｎＴＶ方式コントローラのディジタル署名である暗号化された部分が平文データに依存するデータ上にある。この段階で、プロデューサ／サーバーは、Ｓだけを使用するか、或いは、署名の他に、署名の検査をより容易に行なうため付加データ（例えば、Ｑ１及びＱ２）を追加するかどうかを選択できる。

【００５６】プロデューサ／サーバーは、平文と署名Ｓの間に、４バイトの情報と、場合によっては、検査中に役に立つＳ以外の情報を追加する必要がある。４バイトの情報には、フラグ用のフィールドと、署名と補助情報からなるデータの総数のサイズ用のフィールドとが含まれている。上記二つのフィールドのサイズは以下の通りである。

証明署名情報フラグ長(CERTIFICATE__SIGNATURE __INFO__FLAGS __LENGTH)
２バイト

証明署名サイズ長(CERTIFICATE__SIGNATURE __SIZE__LENGTH) ２バイト

一つのフラグ、ＲＳＡ３方式補助（ＲＳＡ__３__ＡＳＳＩＳＴ）フラグだけが現在定義されている。セットされた場合、署名Ｓの他に、上記二つの商Ｑ１及びＱ２である補助情報がある。上記フラグは：

ＲＳＡ３方式補助(RSA__3 __ASSIST)
(0x8000)

のように定義されている。

【００５７】ここまでは、モジュールレベルの暗号化の状態を説明した。この暗号化は、伝搬パケットレベルの別の暗号化と重ねられる場合がある。即ち、各モジュールが伝送用の伝搬パケットのペイロードに分割されたとき、ペイロードが認証処理とは無関係に暗号化される。システムの一般的な説明に戻ると、例えば、電話モデムによるプロバイダとレシーバの間の双方向通信は、例えば、ＲＳＡ方式、又は、データ暗号化標準ＤＥＳの暗号化法を用いる暗号化通信を組み込む。セッション鍵は、公開鍵暗号化を用いてセットアップされる。アプリケーションは、通信したいサーバーの公開鍵の証明されたバージョンを示す必要がある。セッション鍵は、アプリケーションプロバイダのＩＤが、証明時のサーバーＩＤと一致したときに限り確立され、鍵の交換は、証明に含まれた公開鍵を用いる。

【００５８】図８には、逆伝搬パケットプロセッサの素子を含むＡＶＩ信号受信器又はＩＲＤの一部がブロック形式で示されている。信号は、アンテナ８０によって検出され、受信された信号の中から特定の周波数バンドを抽出し、ベースバンド多重化パケット信号を提供する同調検波器８１に供給される。周波数バンドは、従来の方法で、ＩＲＤシステムコントローラ８９（以下、ＩＲＤコントローラと呼ぶ）を介してユーザによって選択される。名目上、放送ＡＶＩ信号は、例えば、リードーソロモン方式の前方誤差補正（ＦＥＣ）符号化を用いて誤り符号化される。ベースバンド信号は、かくして、前方誤差補正（ＦＥＣ）復号化器８２に供給される。ＦＥＣ復号化器８２は、受信ビデオと同期し、図３に示されたタイプの信号パケットのストリームを提供する。ＦＥＣ復号化器８２は、規則的な間隔、或いは、例えば、メモリコントローラ８７による要求に応じて、パケットを提供する。何れの場合でも、パケットのフレーミング又は同期信号は、各パケット情報がＦＥＣ復号化器８２から転送される時間を示すＦＥＣ回路によって提供される。

【００５９】ただ一つのＡＶＩ信号からのパケットが同時に受信器で処理される。この例の場合、ユーザは選択すべきパケットが分からない場合を想定している。この情報は番組ガイドに含まれ、番組ガイドは、夫々のサービスチャンネル識別子ＳＣＩＤを介して番組の信号成分と相互関係を有するデータからなる特別の番組である。番組ガイドは、夫々の番組のオーディオ、ビデオ及びデータ成分を各番組に対し含むリストである。番組ガイド（図２のパケットＤ４）は固定のサービスチャンネル識別子ＳＣＩＤが割り当てられている。受信器に電力が供給されたとき、ＩＲＤコントローラ８９は、番組ガイドに関係したサービスチャンネル識別子ＳＣＩＤを、マッチドフィルタのバンクであるサービスチャンネル識別子（ＳＣＩＤ）検出器８４にロードするようプログラムされている。番組案内のサービスチャンネル識別子ＳＣＩＤが検出されたとき、メモリコントローラ８７は、ＩＲＤコントローラで使用するため、対応するパケットのペイロードをメモリ８８内の所定の場所に供給するよう条件付けられている。

【００６０】ＩＲＤコントローラは、インタフェース９０を介するユーザからのプログラミングコマンドを待機する。インタフェース９０は、例えば、キーボードとして表わされているが、通常の遠隔制御器又は受像機の前面パネルスイッチでも構わない。ユーザは、（アナログＴＶシステムの呼び名で）チャンネル４に供給された番組の可視化を要求する。ＩＲＤコントローラ８９は、チャンネル４の番組成分の各サービスチャンネル識別子ＳＣＩＤに関しメモリ８８にロードされた番組ガイドリストを走査し、かかるサービスチャンネル識別子ＳＣＩＤをサービスチャンネル識別子検出器８４にロードするようプログラムされている。

【００６１】所定のプログラムに対しオーディオ、ビデオ又はデータプログラム成分からなる受信されたパケットは、最終的に、各オーディオプロセッサ９３、ビデオプロセッサ９２、又は、補助データプロセッサ９１（９４）、シグナルプロセッサに供給されなければならない。データは、比較的一定のレートで受信されるが、シグナルプロセッサは、名目上、例えば、夫々の圧縮解除のタイプに従ってバーストした入力データを要求する。図８の例示的なシステムは、最初に、夫々のパケットをメモリ８８内の所定の記憶場所に供給する。次いで、夫々のプロセッサ９１乃至９４がメモリ８８からの成分のパケットを要求する。メモリを介して成分を供給することにより、所望の信号のデータレートの緩衝又は減速の手段が得られる。

【００６２】オーディオ、ビデオ及びデータパケットは、シグナルプロセッサが成分データを容易にアクセスできるように夫々の所定の記憶場所にある。夫々の成分のパケットのペイロードは、対応するサービスチャンネル識別子ＳＣＩＤと、サービスチャンネル識別子検出器によって供給された制御信号との関数として適当な記憶領域にロードされる。

【００６３】各信号パケットは、前方誤差補正復号化器８２から信号スクランブル解除器８６を介してメモリコントローラ８７に結合される。信号のペイロードだけがスクランブルされ、パケットヘッダはスクランブル解除器によって変更されることなく送られる。パケットのスクランブルを解除すべきかどうかは、パケットの接頭部のＣＦフラグ（図３を参照のこと）によって判定され、そのパケットがスクランブル解除されるべき方法がＣＳフラグによって指令される。上記パケットスクランブリングは、上記アプリケーションモジュールの秘密処理とは無関係である。スクランブル解除された装置は従来の解読器で実現することが可能であり、受信された証明と、必要に応じてそれ以外のデータの解読を行なうため利用される。しかし、以下の伝送されたアプリケーションの説明において、解読は他の装置によって行なわれる。

【００６４】ＡＶＩシステムは、ＡＶＩ信号のＰＣ－データ部と動作可能な多数の装置を含む。例えば、図８において、補助１プロセッサＡＵＸ１と、補助２プロセッサＡＵＸ２の両方は、ＡＶＩ信号のＰＣ－データ部に応答する。補助１プロセッサは、伝送された株価市場データを検出し、伝送された双方向アプリケーションで上記株価市場データを処理するため設けられたパーソナルコンピュータＰＣでもよい。補助２プロセッサは、双方向の衝動買いアプリケーションを伝送された双方向の広告と組み合わせて行なうため設けられたテレビジョンシステムでもよい。双方向性は、図８に示されたシステムと相互接続された電話モデム（図示しない）を用いて容易に実現することができることに注意が必要である。その上、ＩＲＤコントローラ８９は、特に、システム保守のため伝送されたアプリケーションを処理、実行するようプログラムされている。伝送された双方向アプリケーションの実行に関係した受信器の機能は、伝送されたアプリケーションと動作するＩＲＤコントローラ８９の文脈で説明される。双方向性とは、ユーザがプロバイダと相互作用することを必ずしも意味する訳ではなく、それが双方向性の一つの面であるということに注意する必要がある。更に、双方向性は、ユーザが、特に、教育番組の領域で、伝送されたアプリケーションに従ってシステムのユーザ端で信号／システムに影響を与え得るという概念を含んでいる。

【００６５】図９には、図８のＩＲＤコントローラが詳細に表わされている。ＩＲＤコントローラ８９は、ハッシュ関数プロセッサ９６と、解読器９７と、モデム９８と、消去プログラム可能ロム（ＥＰＲＯＭ）９９と共に示されている。ハッシュ関数発生器９６及び解読器９７は、ハードウェア又はソフトウェアで実現可能である。コントローラプロセッサμＰＣは、一般的なシステム命令をプログラミングするためランダムアクセスメモリＲＡＭと及び読み出し専用メモリＲＯＭを含んでいる。他のシステム命令は、ＥＰＲＯＭ９９に格納されている。ＲＯＭ及びＥＰＲＯＭは、製造時にプログラミングされているので、システムは動作可能である。しかし、上記例の場合、ＥＰＲＯＭは、システム機能を更新するため、双方向の伝送されたプログラムを用いて再プログラミングしてもよい。

【００６６】製造時に、受信器が使用されていない午前中の午前１時と午前４時の間にシステム保守サービスチャンネル識別子ＳＣＩＤを探すようシステムがプログラミングされているので、システムプロバイダが新しいシステム強化で夫々の受信器を更新できる場合を想定する。受信器が使用されていない午前中の午前１時と午前４時の間に、コントローラプロセッサは、サービスチャンネル識別子検出器がシステム保全サービスチャンネル識別子を含むパケットを探すようサービスチャンネル識別子検出器をプログラムし、プログラムデータを受けるためメモリ８８を準備する。プログラムモジュール検出

の一例が図１０に示されている。

【００６７】サービスチャンネル識別子の検出と、メモリの準備のためのプログラミングは、スタートアップ処理（ステップ１００）の一部である。サービスチャンネル識別子検出器がプログラムされた後、システムは、システム保全サービスチャンネル識別子を含むパケットが検出されるまでアイドル状態である（ステップ１０２）。このようなパケットが検出されたとき、そのパケットが伝送ユニット又はモジュールヘッダを含んでいるかどうかを判定するためテストされる（ステップ１０４）。否定的に判定された場合、パケットは廃棄され、システムは次のアプリケーションパケットを待つ（ステップ１０２）。あらゆるアプリケーションプログラムをロードするため必要な情報は、プログラム自体（ＴＵヘッダ又はディレクトリモジュールヘッダ）に格納されているので、システムは、適当なヘッダ情報を含むパケットが得られるまで、検出されたパケットをロードしない。適当なパケットが検出されたとき、そのペイロードがメモリ８８にロードされる（ステップ１０６）。システムは、次の保全パケットを待機し（ステップ１０８）、次の保全パケットが検出されたとき、メモリ８８にロードする（ステップ１１０）。各パケットがメモリにロードされた後、完全なモジュールがロードされたかどうかを判定するためテストが行なわれる（ステップ１１２）。モジュールが完全ではない場合、システムは次のパケットを待機するため、ステップ１０８に戻る。モジュールが完全である場合、その旨がリステイングに記録される（ステップ１１４）。

【００６８】次に、完成したモジュールがディレクトリモジュールであるかどうかを判定するためテストが行なわれる（ステップ１１６）。ディレクトリモジュールであるならば、システムは、直ぐにアプリケーションプロバイダの認証を試みる。ディレクトリモジュールに添付された証明が解読され（ステップ１２２）、その内容が検査される（ステップ１２４）。証明の内容が認証されなかった場合、認証されないプロバイダが検出されたことをユーザに通知するため警告表示が作動される（ステップ１３０）。この点で、上記ステップの代わりに、ａ）ステップ１００で処理を再スタートするステップ；ｂ）処理を２４時間停止するステップ；ｃ）ディレクトリモジュールを廃棄し、次のディレクトリモジュールを待機するステップ等を含む多数の別のステップが実施可能である。図１１は、認証処理を詳細に表わす図である。ステップ１１６のテストでディレクトリモジュールが検出された場合、モジュールに追加された証明及び暗号化されたハッシュの値がアクセスされる（ステップ１２２１）。証明は解読器９７に供給され、予め各受信器に配付され、受信器に記憶されたＡＶＩシステムコントローラの公開鍵を使用して解読される（ステップ１２２２）。解読された証明は、コントローラプロセッサに供給される（ステップ１２４１）。コントローラプロセッサμＰＣは、ＥＰＲＯＭから対応する項目を取り出し、関連する対応項目と比較する（ステップ１２４２）。例えば、証明には、許可されたＩＤのリストと比較される識別子ＩＤが含まれている。更に、証明は、現在の日時と比較される満了日時等を含んでいる。比較される項目が受信器に記憶された対応する項目と検査された場合（ステップ１２４３）、証明内で伝送されたアプリケーションプロバイダの公開鍵が解読器に供給され、ディレクトリモジュールに追加された暗号化ハッシュの値を解読し（ステップ１２４４）、或いは、アプリケーションプロバイダによって供給された他の暗号化データを解読するため使用される。この際に、ディレクトリモジュール全体が暗号化されているならば、アプリケーションプロバイダの公開鍵が解読器に供給されている間に、メモリから取り出され、解読される。一方、比較項目が認証されないことが判明し、或いは、証明の期限が満了している場合には、警告が表示される（ステップ１３０）。

【００６９】アプリケーションプロバイダが認証できることが判明した場合、ディレクトリモジュールがハッシュ関数素子９６に供給され、ハッシュされ（ステップ１２６）、ハッシュの値がコントローラプロセッサμＰＣ内で、ディレクトリモジュールに追加された解読後のディレクトリモジュールのハッシュの値と比較される（ステップ１２８）。好ましい実施例の場合、例えば、“ＯｐｅｎＴＶ（登録商標）”のようなシステムコントローラ／プロバイダと関係した所定のテキストのアスキー形式のバージョンが、ハッシングの前に各モジュールに追加されるので、各ハッシュの値は、例えば、Ｈ（ＯｐｅｎＴＶ（登録商標）＋モジュール）と一致する。このことがメモリ８８に付属したボックスＯＴＶによって示されている。これは、例えば、テキスト“ＯｐｅｎＴＶ（登録商標）”のディジタルバージョンが、メモリ８８に記憶され、メモリから読み出されるとき、ディレクトリモジュールと多重化されることを意味している。ハッシュの値が一致しないとき、ディレクトリモジュールは誤りを含んでいると考えられ、メモリから削除され、モジュールが先にロードされていたという事実が（ステップ１１２で作成された）リスティングから消去され（ステップ１３４）、システムは次のパケットを待つためステップ１０８に戻る。

【００７０】ディレクトリモジュールのハッシュの値が追加されたハッシュの値と符合する場合、各プログラムモジュールのハッシュの値が、受信されたプログラムモジュールの完全性を検査する際に使用するためディレクトリから引き出される（ステップ１２９）。システムはステップ１１８に飛び越し、全てのプログラムモジュールがメモリにロードされたかどうかをテストする。未だロードが完了していない場合、次のモジュールへのメモリアドレス指定が準備され、システムは次の適当なパケ

ットを待機するためステップ１０８に戻る。

【００７１】ステップ１１８におけるテストによって、アプリケーションプログラムがメモリに完全に記憶されたことが示された場合、夫々のプログラムモジュールは、伝送の完全性が検査される。夫々のモジュールはメモリから得られ（ステップ１３６）、ハッシュ関数素子９６に供給され、ハッシュされる（ステップ１３８）。夫々のハッシュの値は、コントローラプロセッサμＰＣ内で、ディレクトリモジュール内の伝送されたハッシュの値と比較され（ステップ１４０）、或いは、テストの条件下で、特定のモジュールに追加される。ハッシュの値が符合しない場合、上記モジュールは誤りを含んでいると考えられ、廃棄される（ステップ１５０，１５２）。ハッシュの値が符合するとき、全てのモジュールが検査されたかどうかを判定するためテストが行なわれる（ステップ１４２）。全てのモジュールがテストされたならば、完全な秘密性が符合したアプリケーションがメモリ内に存在するかどうかを判定するため検査が行なわれる（ステップ１４６）。完全なアプリケーションが存在しない場合、システムはステップ１２０に戻り、新しいモジュールのローディングを開始する。アプリケーションが完全である場合、そのアプリケーションが実行される（ステップ１４８）。上記例の場合、プログラムは、コントローラプロセッサμＰＣに、プログラムデータモジュール内の特定のデータをアクセスし、伝送されたデータでＥＰＲＯＭを再プログラミングするよう命令する。

【００７２】システムは、実行が開始された後、伝送された信号からプログラムパケットを抽出し続けるようプログラムされている。受信時に、夫々のヘッダは、バージョン番号が検査される。特定のモジュールのバージョン番号が変化した場合、このモジュールはハッシュ処理をされ、ハッシュの値が符合する場合、新しいバージョン番号を含む上記モジュールが前の対応するモジュールを置き換える。

【００７３】

【発明の効果】上記の如く、受信装置内の別個の装置は、特定の伝送されたアプリケーションを利用し、アプリケーションの実行前に必要な秘密化処理を行なうようプログラミングされている。好ましい実施例において、プログラミング又はハードウェアの重複を回避するため、秘密化処理は統合形の受信装置の復号化器（ＩＲＤ）コントローラによって行なわれる。ＩＲＤコントローラは、秘密化処理を番組ガイド内に格納された情報によって実行する必要があるときに警告される。

【図面の簡単な説明】

【図１】本発明の一面を具現化する双方向ＴＶ信号符号化システムのブロック図である。

【図２】オーディオビジュアルインタラクティブ信号の一例の一部分を表わす図である。

【図３】伝搬パケットの一例を表わす図である。

【図４】本発明を説明するために使用されるオーディオビジュアルインタラクティブアプリケーションの一例のフォーマットを表わす図である。

【図５】伝送ユニットヘッダの一例の内容の表である。

【図６】本発明を具現化するオーディオビジュアルインタラクティブアプリケーションのディレクトリモジュールの一例の内容の表である。

【図７】本発明を具現化するオーディオビジュアルインタラクティブアプリケーションに安全／保護を与える処理を表わすフローチャートである。

【図８】本発明を具現化する受信器装置の一例のブロック図である。

【図９】図８の装置のプロセッサとして実装可能なプロセッサの一例の拡大ブロック図である。

【図１０】本発明の受信器の一実施例を表わす図８の受信器装置の一部分の動作を表わすフローチャートである。

【図１１】本発明の一実施例である証明の認証処理の一例のフローチャートである。

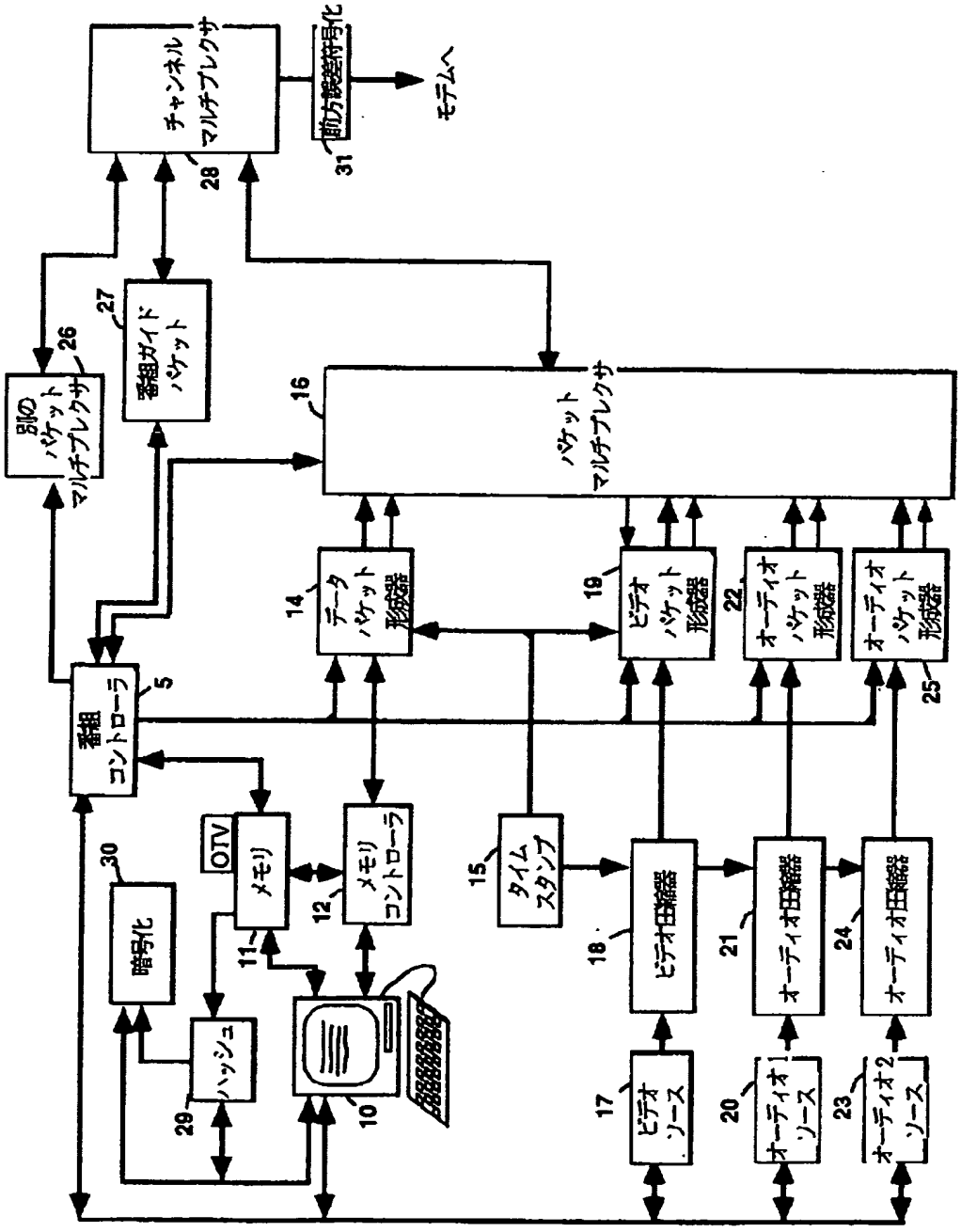
【図１２】本発明による好ましいディレクトリモジュールのフォーマットを表わす図である。

【符号の説明】

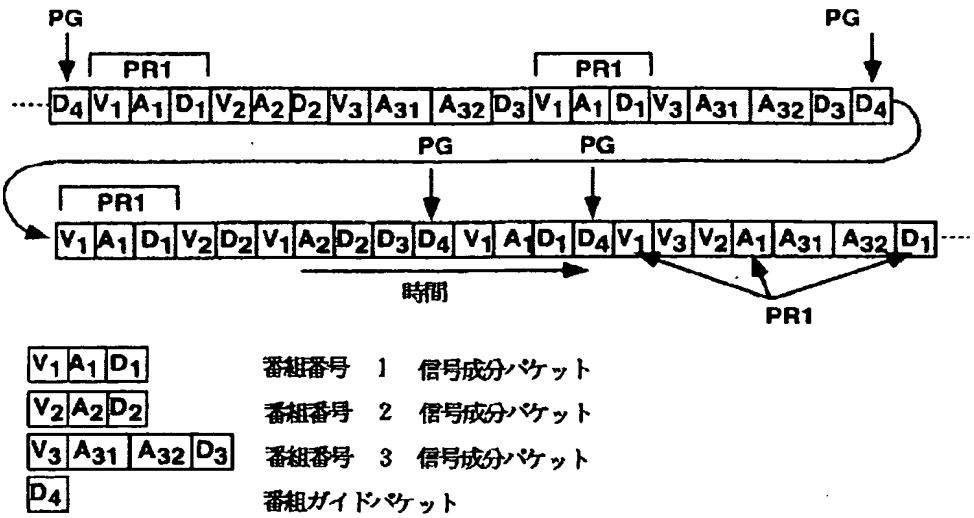
５　システム番組コントローラ
１０　インタラクティブ成分ソース
１１，８８　メモリ
１２，８７　メモリコントローラ
１４　コード／データパケットプロセッサ
１５　タイミング素子
１６，２６　パケットマルチプレクサ
１７　ビデオソース
１８　ビデオ信号圧縮器
１９　ビデオパケット形成器
２０，２３　オーディオソース
２１，２４　アーディオ信号圧縮器
２２，２５　オーディオパケット形成器
２７　番組案内パケット
２８　チャンネルマルチプレクサ
２９，９６　ハッシュ関数プロセッサ
３０　暗号化器
３１　前方誤差符号化（ＦＥＣ）信号インターリーブ装置
８０　アンテナ
８１　同調検波器
８２　前方誤差補正（ＦＥＣ）復号化器
８４　サービスチャンネル識別子（ＳＣＩＤ）検出器
８６　信号スクランブル解除器
８９　ＩＲＤシステムコントローラ
９０　インタフェース
９１　補助１プロセッサ

９２　ビデオプロセッサ
９３　オーディオプロセッサ
９４　補助２プロセッサ
＊９７　解読器
９８　モデム
＊　９９　ＥＰＲＯＭ

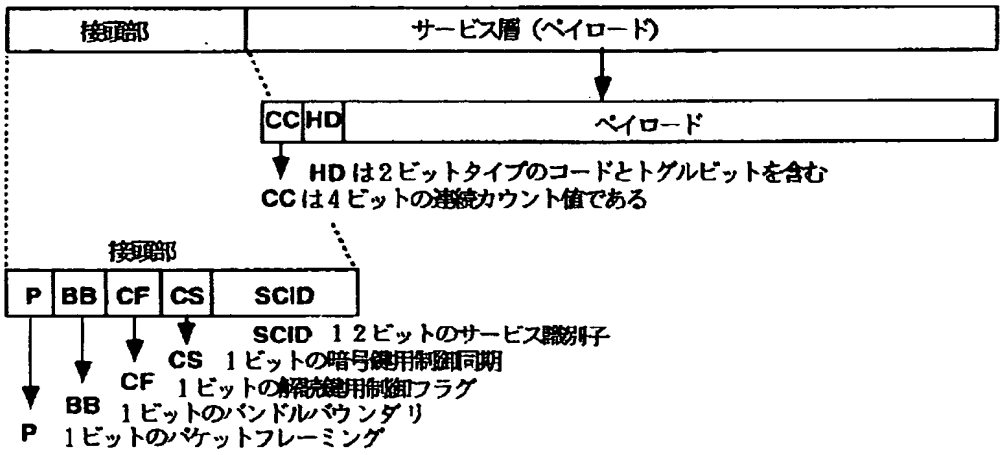
【図１】



【図２】



【図３】

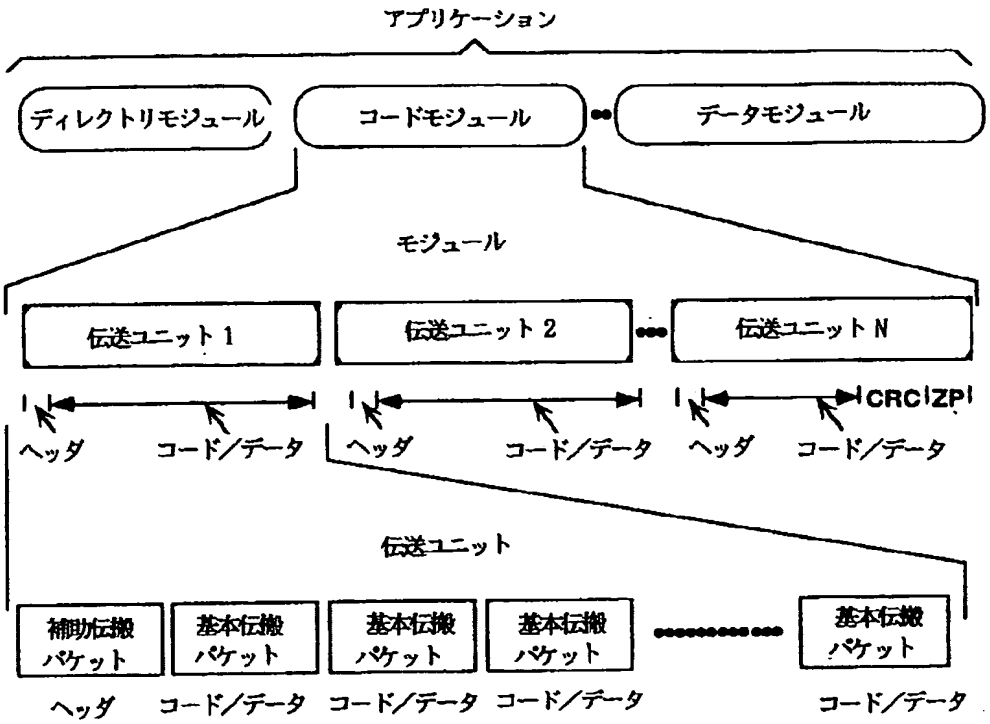


【図５】

表　I

ビット数	機能
16	モジュール識別子
32	CRCを含むモジュール内の総バイト数
32	モジュールバージョン番号
32	モジュール伝送ユニットバイトオフセット
32	伝送ユニットの（バイト）長
XX	予備

【図４】

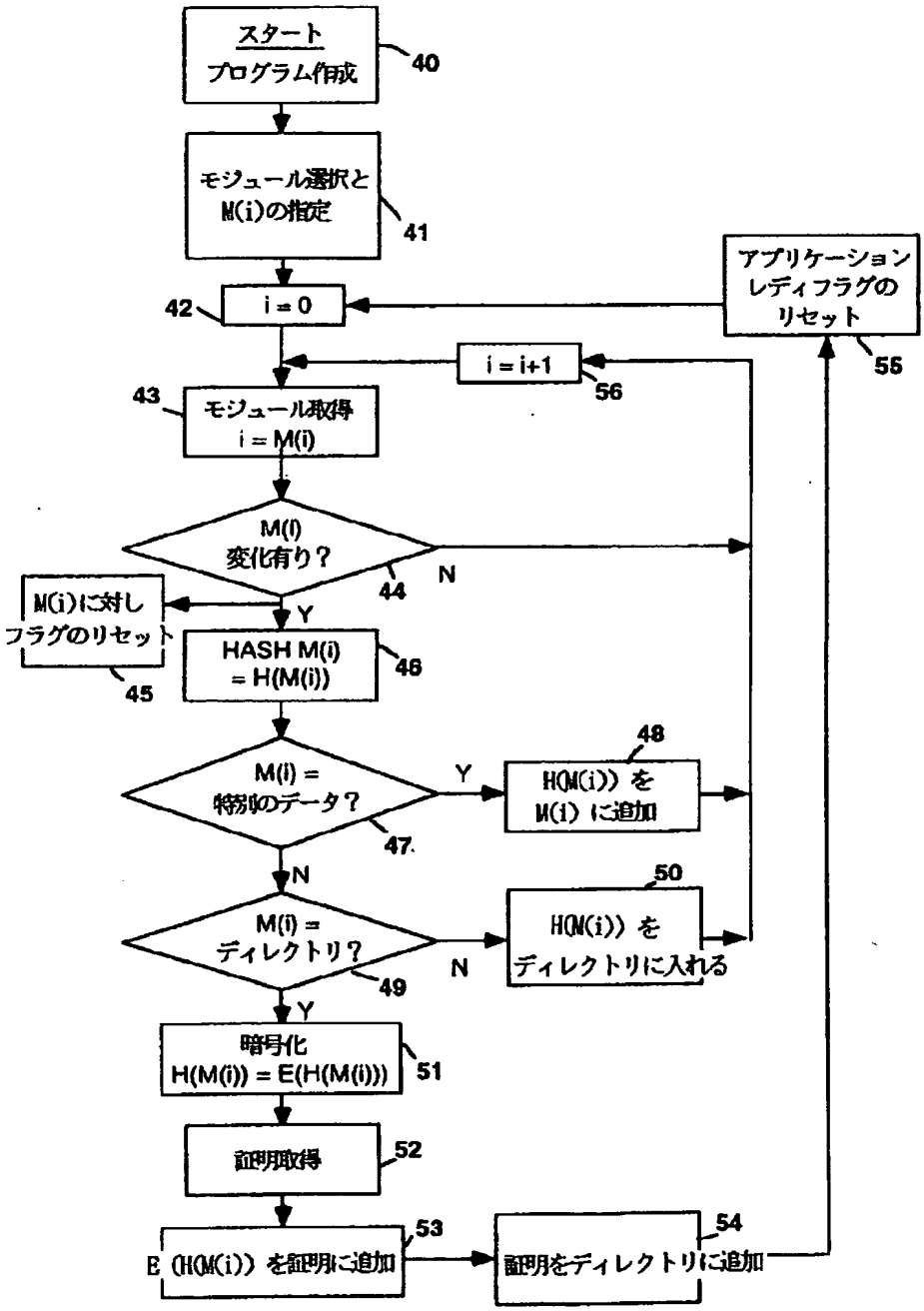


【図６】

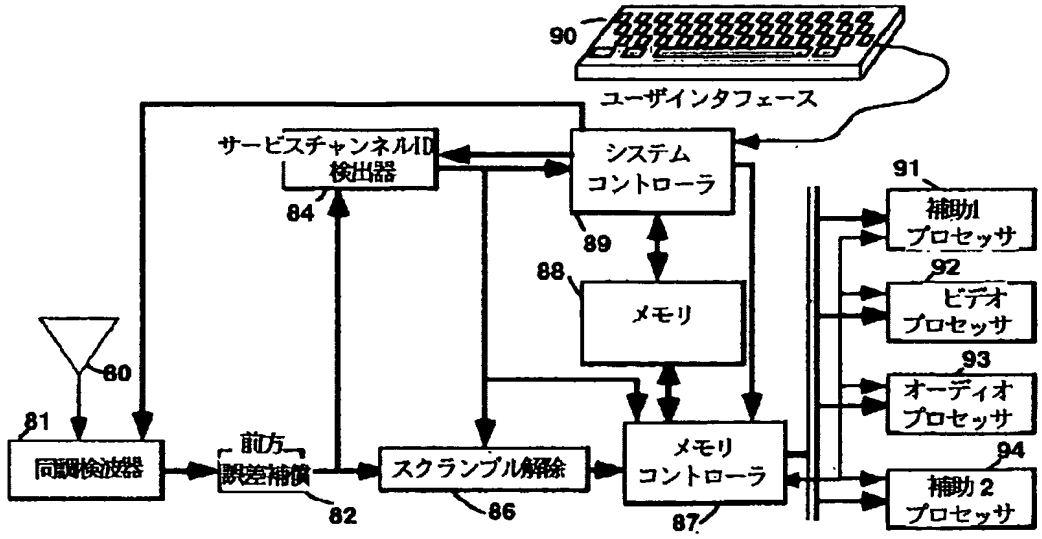
表 Ⅱ

ビット数	機能
32	アプリケーション識別子(ＡＩＤ)
YY	アプリケーションタイプ
ZZ	アプリケーション限定子
32	アプリケーション用復号化器メモリ必要量
16	総モジュール数
XX	第１の秘密情報
	各モジュールに対して
16	モジュールストリングテーブルへのポインタ
16	モジュール識別子
32	モジュールバージョン番号
32	ＣＲＣを含むモジュール長
32	復号化器メモリ必要量（コードモジュールの場合）
32	他のフラグ
XX	モジュール名の文字列テーブル，文字列はヌルで終端
NN	別の秘密情報
署名付き証明	
ハッシュ	

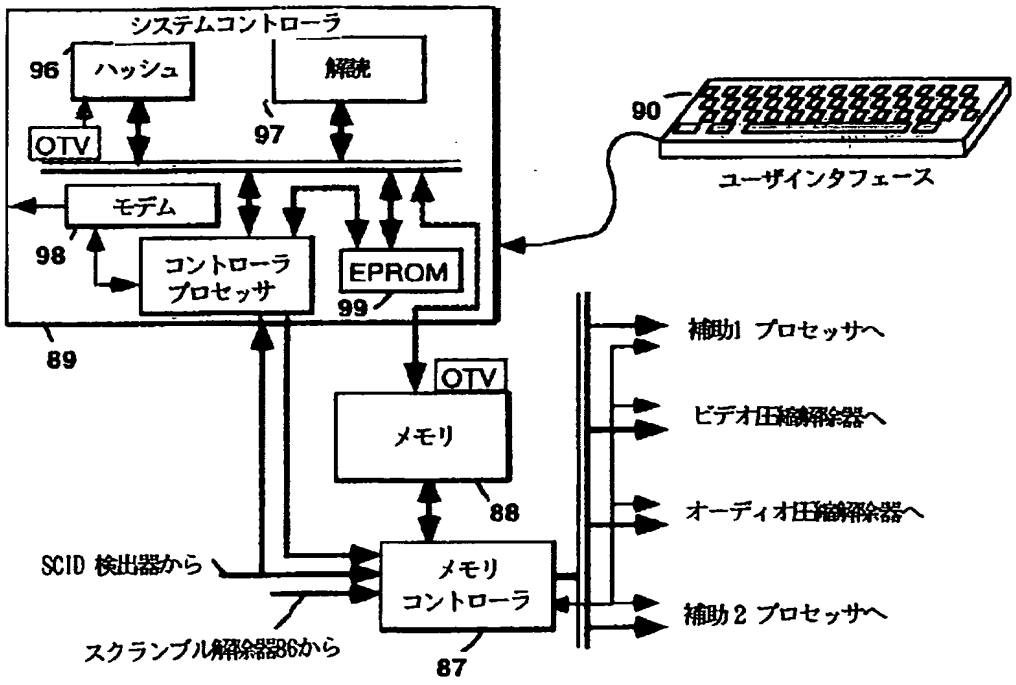
【図７】


スタート
プログラム作成
40
モジュール選択と
M(i)の指定
41
i = 0
42
アプリケーション
レディフラグの
リセット
55
i = i+1
56
43
モジュール取得
i = M(i)
M(i)
変化有り？
44
N
Y
M(i)に対し
フラグのリセット
45
HASH M(i)
= H(M(i))
46
M(i) =
特別のデータ？
47
Y
48
H(M(i)) を
M(i) に追加
N
M(i) =
ディレクトリ？
49
N
50
H(M(i)) を
ディレクトリに入れる
Y
暗号化
H(M(i)) = E(H(M(i)))
51
証明取得
52
E (H(M(i)) を証明に追加
53
54
証明をディレクトリに追加

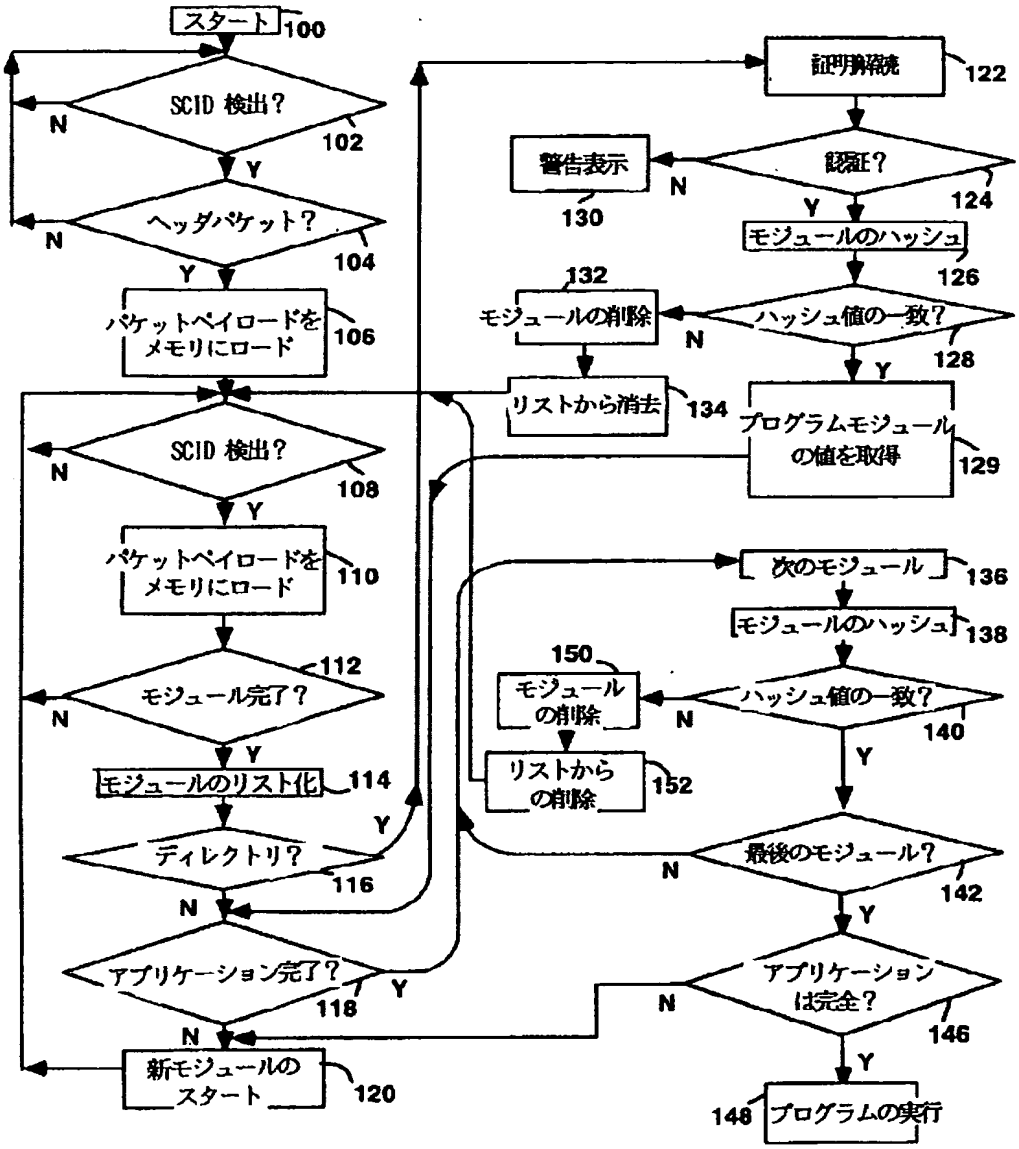
【図８】


90
ユーザインタフェース
サービスチャンネルID検出器
84
システムコントローラ
89
91
補助1プロセッサ
88
メモリ
92
ビデオプロセッサ
93
オーディオプロセッサ
80
81
同調検波器
前方誤差補償
82
スクランブル解除
86
メモリコントローラ
87
94
補助2プロセッサ

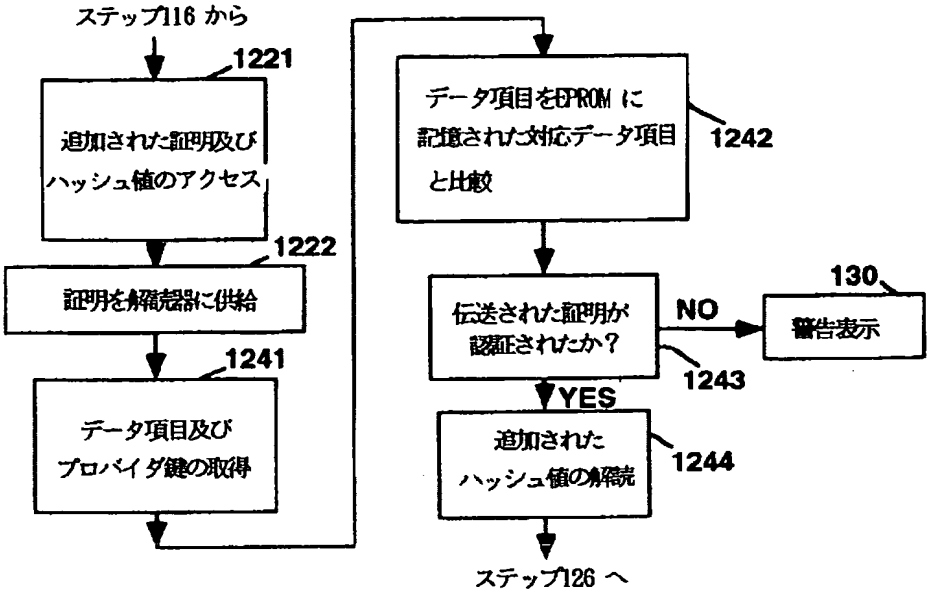
【図９】


システムコントローラ
96
ハッシュ
解読
97
OTV
モデム
98
コントローラプロセッサ
EPROM
99
89
90
ユーザインタフェース
補助1 プロセッサへ
ビデオ圧縮解除器へ
オーディオ圧縮解除器へ
補助2 プロセッサへ
OTV
メモリ
88
SCID 検出器から
メモリコントローラ
スクランブル解除器86から
87

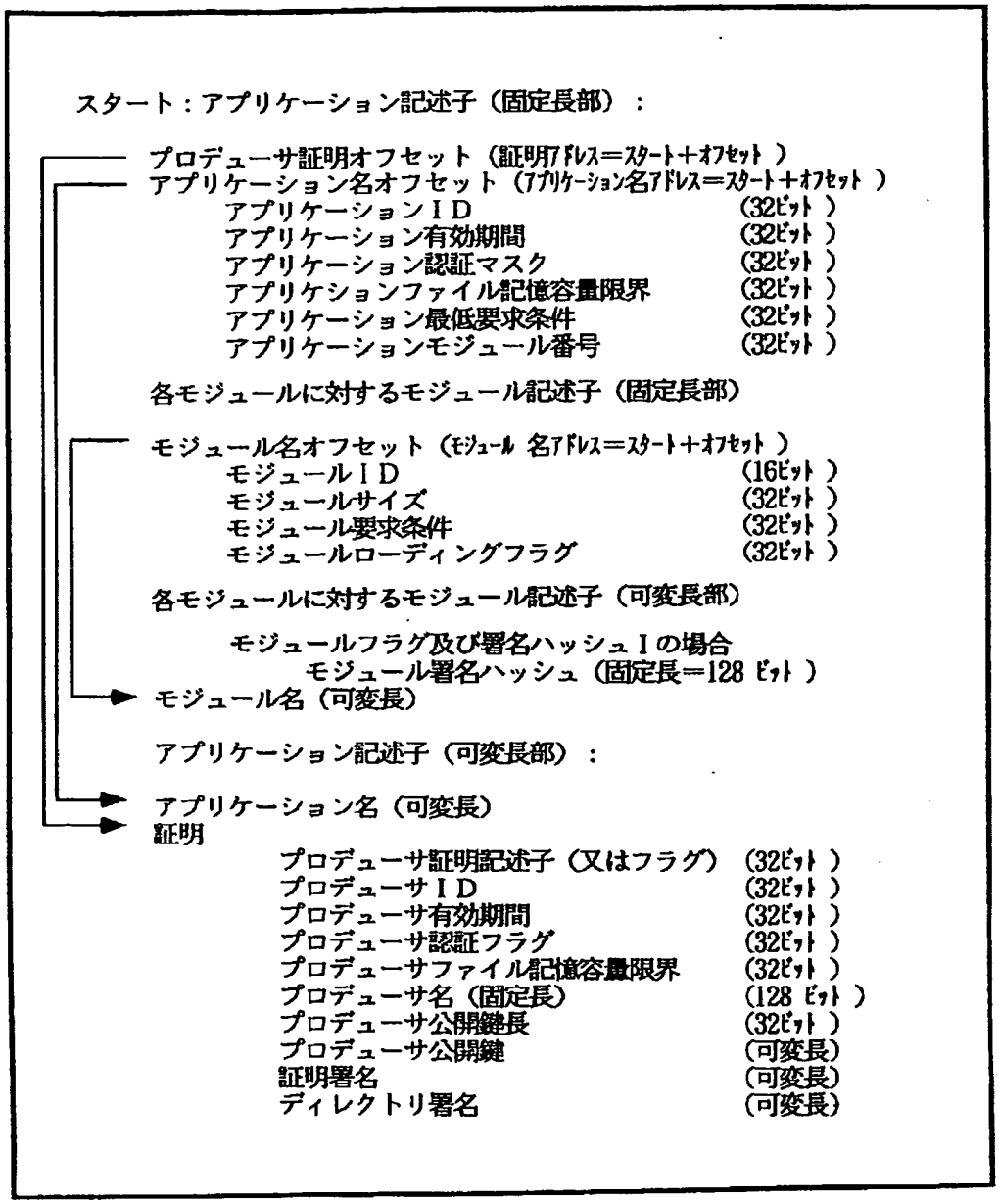
【図１０】


スタート
100
SCID 検出?
102
N
Y
ヘッダパケット?
104
パケットペイロードを
メモリにロード
106
SCID 検出?
108
パケットペイロードを
メモリにロード
110
モジュール完了?
112
モジュールのリスト化
114
ディレクトリ?
116
アプリケーション完了?
118
新モジュールの
スタート
120
証明鍵読
122
認証?
124
警告表示
130
モジュールのハッシュ
126
ハッシュ値の一致?
128
132
モジュールの削除
リストから消去
134
プログラムモジュール
の値を取得
129
次のモジュール
136
モジュールのハッシュ
138
ハッシュ値の一致?
140
150
モジュール
の削除
リストから
の削除
152
最後のモジュール?
142
アプリケーション
は完全?
146
プログラムの実行
148

【図１１】


ステップ116 から
1221
追加された証明及び
ハッシュ値のアクセス
1222
証明を解読器に供給
1241
データ項目及び
プロバイダ鍵の取得
データ項目をEPROM に
記憶された対応データ項目
と比較
1242
伝送された証明が
認証されたか？
NO
130
警告表示
1243
YES
追加された
ハッシュ値の解読
1244
ステップ126 へ

【図１２】



フロントページの続き

(72)発明者　パンカジ　ロハトギ
アメリカ合衆国　カリフォルニア州
94086　サニーヴェール　ヴィセンテ・ド
ライヴ　1256　アパートメント・エイチ

(72)発明者　ヴィンセント　デュロ
アメリカ合衆国　カリフォルニア州
90291　ヴェニス　シャーマン・カナル
219

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.